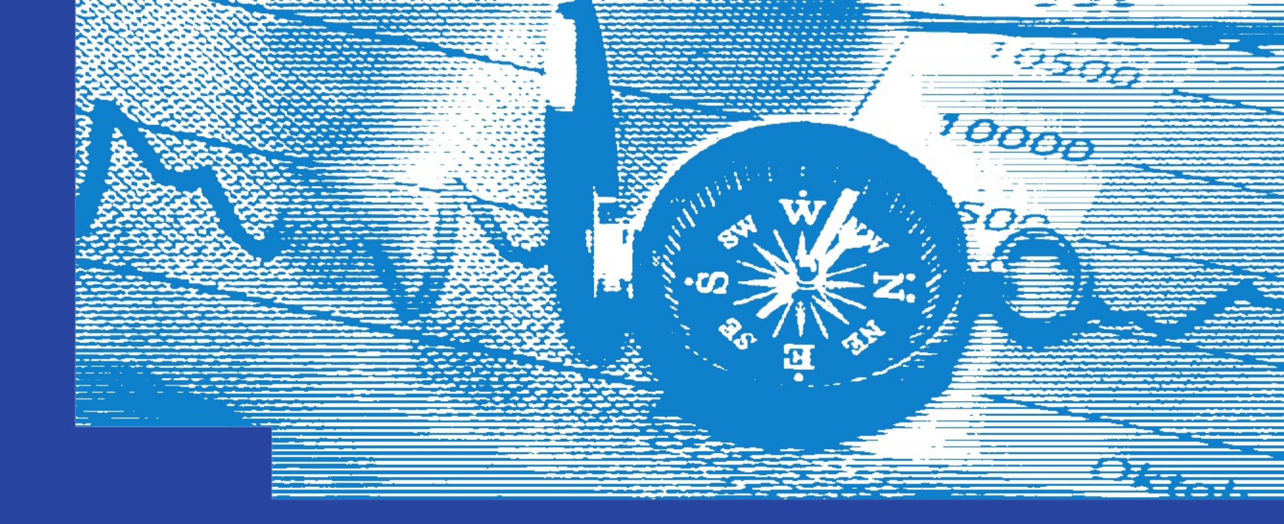


Gregor Wecker | Hendrik van Laak (Hrsg.)

Compliance in der Unternehmerpraxis

Grundlagen, Organisation und Umsetzung



Gregor Wecker | Hendrik van Laak (Hrsg.)

Compliance in der Unternehmerpraxis

Gregor Wecker | Hendrik van Laak (Hrsg.)

Compliance in der Unternehmerpraxis

Grundlagen, Organisation und Umsetzung



Bibliografische Information Der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<http://dnb.d-nb.de> abrufbar.

1. Auflage 2008

Lektorat: RA Andreas Funk

Der Gabler Verlag ist ein Unternehmen von Springer Science+Business Media.
www.gabler.de



Umschlaggestaltung: Nina Faber de.sign, Wiesbaden
Druck und buchbinderische Verarbeitung: Wilhelm & Adam, Heusenstamm
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.
Printed in Germany

ISBN 978-3-8349-0971-8

Vorwort

Compliance verstanden als Gesamtkonzept organisatorischer Maßnahmen, mit denen die Rechtmäßigkeit der unternehmerischen Aktivitäten gewährleistet werden soll, ist kein (reines) Rechtsproblem. Die Identifikation der (rechtlichen) Risiken bildet nur einen – wenn auch einen wichtigen – Ausgangspunkt, von dem aus der Handlungsbedarf ermittelt und die entsprechenden organisatorischen Maßnahmen im Unternehmen entwickelt und umgesetzt werden, um diesen Risiken zu begegnen.

Dass der Aufbau und die Implementierung einer derartigen Organisation ein schwieriger, umfangreicher und auch kostspieliger Prozess sein kann, muss hier nicht besonders betont werden. Gleichwohl hat der Deutsche Corporate Governance Kodex in Ziff. 4.1.3 nunmehr die Compliance ausdrücklich als Geschäftsleitungsaufgabe verankert und macht durch seine sprachliche Darstellung deutlich, dass er Compliance als geltendes Gesetzesrecht versteht. Wenn der Deutsche Corporate Governance Kodex auch grundsätzlich nur für börsennotierte Aktiengesellschaften relevant ist, darf dies nicht darüber hinwegtäuschen, dass die Pflicht zu einer entsprechenden Organisation auch nicht börsennotierte Aktiengesellschaften und Unternehmen anderer Rechtsformen trifft.

Eine solche Verpflichtung ist Anlass genug, sich mit der Compliance im eigenen Unternehmen zu befassen. Wichtig dürfte aber ein weiterer Aspekt sein, der in der weiten Compliance-Diskussion unberechtigterweise häufig in den Hintergrund gedrängt wird. Eine gut integrierte Compliance-Organisation erschöpft sich keinesfalls in der Funktion eines „Risikominimierers" oder „Schadens- und Haftungsverhinderers". Vielmehr steigert eine solche Organisation die Unternehmenseffizienz und kann dadurch den Unternehmenserfolg fördern. Die Risikominimierung stellt sich bei zunehmend funktionierenden Compliance-Strukturen lediglich als ein Aspekt und ein Effekt guter Corporate Compliance dar.

Der vorliegende Band will im Kontext verschiedener Schwerpunktbereiche, die sich in der Praxis als besonders „compliance-relevant" erwiesen haben, immer wieder den Schnittpunkt von Rechtspflichten und Unternehmensorganisation beleuchten. Ziel soll es sein, einerseits relevante Pflichten herauszuarbeiten und andererseits den Unternehmen zugleich unternehmensorganisatorische Umsetzungsansätze an die Hand zu geben.

In diesem Zusammenhang gilt der besondere Dank der Herausgeber den Autoren, die ihre aus langjähriger Praxis in den jeweiligen Beratungsschwerpunkten gewonnenen Erkenntnisse haben einfließen lassen und ihre Erfahrungen in diesem Buch einem größeren Interessentenkreis zugänglich machen.

Wir hoffen, den Lesern mit den folgenden Beiträgen Anregungen und Hinweise geben zu können, die ihnen bei ihrer täglichen Arbeit helfen. Das Buch versteht sich als Einstieg in die Problematik mit einer auf das Wesentliche konzentrierten, aktuellen und praxisorientierten Darstellung. Entsprechend beschränken sich die Hinweise zu weiterführender Literatur ganz überwiegend auf Beiträge jüngeren Datums.

Herausgeber und Autoren streben den Dialog mit dem Leser dieses Buches bzw. den Verantwortlichen für Compliance im Unternehmen an. Fragen und Anregungen sind deshalb jederzeit willkommen und können unter vorname.nachname@luther-lawfirm.com direkt an die jeweiligen Autoren oder an die Herausgeber gerichtet werden.

Köln, im März 2008

Dr. Gregor Wecker
Hendrik van Laak

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

A

a.a.O. am angegebenen Ort
Abs. Absatz
AG Die Aktiengesellschaft
AGB Allgemeine Geschäftsbedingungen
AGG Allgemeines Gleichbehandlungsgesetz
AktG Aktiengesetz
AL Ausfuhrliste
AO Abgabenordnung
ArbSchG Arbeitsschutzgesetz
ArbZG Arbeitszeitgesetz
Art. Artikel
ASiG Arbeitssicherheitsgesetz
AuA Arbeit und Arbeitsrecht
AufenthG Aufenthaltsgesetz
Aufl. Auflage
AÜG Arbeitnehmerüberlassungsgesetz
AWG Außenwirtschaftsgesetz
AWR Außenwirtschaftsrecht
AWV Außenwirtschaftsverordnung
Az. Aktenzeichen

B

BAFA Bundesamt für Wirtschaft und Ausfuhrkontrolle
BAFin Bundesanstalt für Finanzdienstleistungsaufsicht
BAKred Bundesaufsichtsamt für das Kreditwesen
BB Betriebs-Berater
BDSG Bundesdatenschutzgesetz
Beschl. Beschluss
betr. betrifft
BetrVG Betriebsverfassungsgesetz
BFH Bundesfinanzhof
BFHE Bundesfinanzhof-Entscheidungen
BGB Bürgerliches Gesetzbuch

BGH Bundesgerichtshof
BGHZ Entscheidungssammlung des Bundesgerichtshofs in Zivilsachen
BI Business Intelligence
BilMoG Bilanzrechtsmodernisierungsgesetz
BKartA Bundeskartellamt
BKR Bank- und Kapitalmarktrecht
BMF Bundesministerium für Finanzen
BMI Bundesministerium des Innern
BSI Bundesamt für Sicherheit in der Informationstechnik
BSIG BSI-Errichtungsgesetz
bspw. beispielsweise
BT-Drucks Bundestagsdrucksachen
bzw. beziehungsweise

C

CC Common Criteria for Information Technology Security Evaluation
CCO Chief Compliance Officer
CIO Chief Information Officer
CobiT Control Objectives for Business Information and Related Technologies
Corp. Corporation
COSO Committee of Sponsoring Organisations of the Treadway Commission
CR Computer und Recht
CSO Chief Security Officer
CSR Corporate Social Responsibility
CWÜ Chemiewaffenübereinkommen

D

D&O Directors and Officers
d. h. das heißt
DB Der Betrieb
DCGK Deutscher Corporate Government Kodex
DoD Department of Defense
DPL Denied Persons List
DSD Duales System Deutschland
DStR Deutsches Steuerrecht
DZWIR Deutsche Zeitschrift für Wirtschaft und Insolvenzrecht

E

e. V. eingetragener Verein
EAR Export Administration Regulations
ebd. ebendort
ECM Enterprise Content Management

EG	Europäische Gemeinschaft
EnSEC	Enterprise Security Management
ERP	Enterprise Resource Planning
EStG	Einkommensteuergesetz
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUR	EURO
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWR	Europäischer Wirtschaftsraum

F

f.	folgende
FBA	Foreign Business Act
ff.	folgende
FIE	Foreign Invested Enterprises
FIPB	Foreign Investment Promotion Board
Fn.	Fußnote
FS	Festschrift

G

GASP	Gemeinsame Außen- und Sicherheitspolitik
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GewO	Gewerbeordnung
GG	Grundgesetz
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	GmbH-Gesetz
GmbHR	GmbH Rundschau
GoB	Grundsätze ordnungsgemässer Buchführung
GoBS	Grundsätze ordnungsgemässer EDV-gestützter Buchführungssysteme
GPSG	Geräte- und Produktsicherheitsgesetz
GRC	Governance Risk Compliance
GWB	Gesetz gegen Wettbewerbsbeschränkungen

H

HGB	Handelsgesetzbuch
HIPAA	Health Insurance Portability and Accountability Act
Hrsg.	Herausgeber

I

i. S.	im Sinne
i.V.m.	in Verbindung mit
ICC	International Chamber of Commerce

ICSID International Center for Settlement of Investment Disputes
IDW Institut der Wirtschaftsprüfer
IKS Internes Kontrollsystem
InsO Insolvenzordnung
IP Intellectual Property
ISA Instrumentation, Systems and Automation Society
ISG Information Security Governance
ISO International Standards Organisation
IStR Internationales Steuerrecht
IT Informationstechnologie
ITIL Information Technology Infrastructure Library
ITRB Information Technology Review Board

J

JZ Juristenzeitung

K

K&R Kommunikation & Recht
kg Kilogramm
KG Kommanditgesellschaft
KonTraG Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KrWaffG Kriegswaffengesetz
KschG Kündigungsschutzgesetz
KWG Kreditwesengesetz

L

LAG Landesarbeitsgericht
LG Landgericht

M

M&A Merger & Acquisition
M.A. Magister Artium
m.w.N. mit weiteren Nachweisen
MAH Mindestanforderungen an das Betreiben von Handelsgeschäften bei Kreditinstituten
MaIR Mindestanforderungen an die Interne Revision
MaK Mindestanforderungen für das Kreditgeschäft
MaRisk Mindestanforderung an das Risikomanagement
MMR Multimedia und Recht
MRC Management Risk Controlling
Mrd. Milliarde
MTCR Missile Technology Control Regime

MüKo Münchener Kommentar

N

NJW Neue juristische Wochenschrift
Nr. Nummer
NSG Nuclear Suppliers Group
NVwZ Neue Verwaltungsrecht-Zeitung
NZA Neue Zeitschrift für Arbeitsrecht
NZA-RR Neue Zeitschrift für Arbeitsrecht - Rechtsprechungsreport

O

ÖBA Bank-Archiv
OEM Original equipment manufacturer
OFT Office of Fair Trading
OHG Offene Handelsgesellschaft
OLG Oberlandesgericht
OSZE Organisation für Sicherheit und Zusammenarbeit in Europa
OwiG Ordnungswidrigkeitengesetz

P

PC Personal Computer
ProdHaftG Produkthaftungesetz
PS Prüfungsstandards

R

RDV Rahmendienstvereinbarung
RegBegr Regierungsbegründung
RIW Recht der Internationalen Wirtschaft
Rn. Randnummer

S

S. Seite
s.u. siehe unten
SAM Steueranwaltsmagazin
SchiedsVZ Die neue Zeitschrift für Schiedsverfahren
SEC Securities and Exchange Commission
SGB Sozialgesetzbuch
SiG Signaturgesetz
SOA Sarbanes-Oxley Act
SOD Segregation of Duties
SOX Sarbanes-Oxley Act
StGB Strafgesetzbuch

StuW Steuern und Wirtschaft

T

t Tonne
TKG Tele-Kommunikations-Gesetz
TMG Telemediengesetz

U

u. ä. und ähnliches
UN United Nations
Urt. v. Urteil vom
USD United States Dollar

V

VAG Versicherungsaufsichtsgesetz
VersR Versicherungsrecht
vgl. vergleiche
VO Verordnung
VVG Versicherungsvertragsgesetz

W

WM Wertpapiermitteilungen
WpHG Wertpapierhandelsgesetz
WTO World Trade Organisation

X

XAM Extensible Access Method
XBRL Extensible Business Reporting Language

Z

z. B. zum Beispiel
ZBB Zeitschrift für Bankrecht und Bankbetriebswirtschaft
ZfIR Zeitschrift für Immobilienrecht
ZGR Zeitschrift für Unternehmens- und Gesellschaftsrecht
ZIP Zeitschrift für Wirtschaftsrecht und Insolvenzpraxis
ZRP Zeitschrift für Rechtspolitik mit Rechtspolitischer Umschau
ZWeR Zeitschrift für Wettbewerbsrecht

Literaturverzeichnis

ADAMS, HEINZ W./JOHANNSEN, DIRK; Das „gerichtsfeste“ Produktionsunternehmen, BB 1996, S. 1017-1021.

ALTMEPPEN, HOLGER; Ungültige Vereinbarungen zur Haftung von GmbH-Geschäftsführern, DB 2000, S. 261-263.

ALTMEPPEN, HOLGER; Zur Disponibilität der Geschäftsführerhaftung in der GmbH, DB 2000, S. 657-661.

BERGMANN, LUTZ/ MÖHRLE, ROLAND/HERB, ARMIN; Datenschutzrecht, Kommentar Bundesdatenschutzgesetz, Loseblatt, Stuttgart, München, Hannover, Berlin, Weimar, Dresden, Stand: Juli 2007.

BERNDT, THOMAS/HOPPLER, IVO; Whistleblowing – ein integraler Bestandteil effektiver Corporate Governance, BB 2005, S. 2623-2629.

BERWANGER, JÖRG/KULLMANN, STEFAN; Interne Revision – Wesen, Aufgaben und rechtliche Verankerung, Wiesbaden 2008.

BREINLINGER, ASTRID/KRADER, GABRIELA; Whistleblowing – Chancen und Risiken bei der Umsetzung von anonym nutzbaren Hinweisgebern im Rahmen des Compliance-Managements von Unternehmen, RDV 2006, S. 60-70.

BÜRKLE, JÜRGEN; Weitergabe von Informationen über Fehlverhalten in Unternehmen (Whistleblowing) und Steuerung auftretender Probleme durch ein Compliance-System, DB 2004, S. 2158-2161.

BÜRKLE, JÜRGEN; Corporate Compliance – Pflicht oder Kür für den Vorstand der AG?, BB 2005, S. 565-570.

BÜRKLE, JÜRGEN; Corporate Compliance als Standard guter Unternehmensführung des Deutschen Corporate Governance Kodex, BB 2007, S. 1797-1801.

DÄUBLER, WOLFGANG/KLEBE, THOMAS/WEDDE, PETER/WEICHERT, THILO; Bundesdatenschutzgesetz, Basiskommentar, 2. Auflage, Frankfurt 2007.

DREHER, MEINRAD; Die kartellrechtliche Bußgeldverantwortlichkeit von Vorstandsmitgliedern: Vorstandshandeln zwischen aktienrechtlichem Legalitätsprinzip und kartellrechtliche Unsicherheit, in: FS Konzen, Tübingen 2006, S. 85-108.

DREHER, MEINRAD; Kartellrechtscompliance in der Versicherungswirtschaft, VersR 2004, S. 1-8.

DREHER, MEINRAD; Kartellrechtscompliance – Voraussetzungen und Rechtsfolgen unternehmens- oder verbandsinterner Maßnahmen zur Einhaltung des Kartellrechts, ZWeR 2004, S. 75-105.

EHRLER, JÜRGEN; Compliance in Universalbanken – Strategien für das Management von Interessenkonflikten, Wiesbaden 1997.

EISELE, DIETER; Insiderrecht und Compliance, WM 1993, S. 1021-1026.
ESCHENBRUCH, KLAUS; Projekt-Compliance, ZfIR 2007, S. 470-475.
FELDHAUS, GERHARD; Umweltschutzsichernde Betriebsorganisation, NVwZ 1991, S. 927-935.
FLEISCHER, HOLGER; Die „Business Judgement Rule“ – Vom Richterrecht zur Kodifizierung, ZIP 2004, S. 685-692.
FLEISCHER, HOLGER; Aktienrechtliche Legalitätspflicht und „nützliche“ Pflichtverletzungen von Vorstandsmitgliedern, ZIP 2005, S. 141-152.
FLEISCHER, HOLGER; Vorstandsverantwortlichkeit und Fehlverhalten von Unternehmensangehörigen – Von einer Einzelüberwachung zur Errichtung einer Compliance-Organisation, AG 2003, S. 291-300.
GOLA, PETER/SCHOMERUS, RUDOLF; BDSG Bundesdatenschutzgesetz, Kommentar, 9. Auflage, München 2007.
GROHNERT, STEPHAN; Rechtliche Grundlagen einer Compliance-Organisation und ausgewählte Fragen der Umsetzung, Hamburg 1999.
HABERSACK, MATHIAS; Gesteigerte Überwachungspflichten des Leiters eines sachnahen Vorstandressorts?, WM 2005, S. 2360-2364.
HAUSCHKA, CHRISTOPH E.; Der Compliance-Beauftragte im Kartellrecht – Absicherungsstrategien für mittelständische Unternehmen und deren Organe, BB 2004, S. 1178-1182.
HAUSCHKA, CHRISTOPH E.; Compliance am Beispiel der Korruptionsbekämpfung, ZIP 2004, S. 877-883.
HAUSCHKA, CHRISTOPH E.; Von Compliance zu Best Practice, ZRP 2006, 258-261.
HAUSCHKA, CHRISTOPH E.; Compliance, Compliance-Manager, Compliance-Programme: Eine geeignete Reaktion auf gestiegene Haftungsrisiken für Unternehmen und Management?, NJW 2004, S. 257-261.
HAUSCHKA, CHRISTOPH E. *(HRSG.)*; Corporate Compliance, München 2007.
HAUSCHKA, CHRISTOPH E.; Corporate Compliance – Unternehmensorganisatorische Ansätze zur Erfüllung der Pflichten von Vorständen und Geschäftsführern, AG 2004, S. 461-475.
HAUSCHKA, CHRISTOPH E.; Ermessensentscheidungen bei der Unternehmensführung, GmbHR 2007, S. 11-16.
HAUSCHKA, CHRISTOPH E.; Die Voraussetzungen für ein effektives Compliance System i.S. von § 317 Abs. 4 HGB, DB 2006, S. 1143-1146.
HAUSCHKA, CHRISTOPH E./GREEVE, GINA; Compliance in der Korruptionsprävention – was müssen, was sollen, was können die Unternehmen tun?, BB 2007, S. 165-173.
HAUSCHKA, CHRISTOPH E./KLINDT, THOMAS; Eine Rechtspflicht zur Compliance im Reklamationsmanagement?, NJW 2007, S. 2726-2729.
HAUSMANINGER, CHRISTIAN/KRETSCHMER, WERNER/OPPITZ, MARTIN; Insiderrecht und Compliance, Wien 1995.
HEFENDEHL, ROLAND; Corporate Governance und Business Ethics: Scheinberuhigung oder Alternativen bei der Bekämpfung der Wirtschaftskriminalität? JZ 2006, S. 199-125.

HERBERT, MANFRED/OBERRATH, JÖRG-DIETER; Schweigen ist Gold? Rechtliche Vorgaben für den Umgang des Arbeitnehmers mit seiner Kenntnis über Rechtsverstöße im Betrieb, NZA 2005, S. 193-199.

HOFFMANN, THOMAS; Rechtliche Schranken interner Informationsflüsse in Kreditinstituten, Studien zum Bank- und Börsenrecht, Baden-Baden 1998.

HUBER, ERICH/SEER, ROMAN; Steuerverwaltung im 21. Jahrhundert: Risikomanagement und Compliance, StuW 2007, S. 355-371.

JANSSEN, HELMUT/WÜSTENFELD, RAINER; Der praktische Nutzen kartellrechtlicher Compliance, Compliance Report, Heft 10, Oktober 2007, S. 5-7.

JANSSEN, HELMUT/VON DIETZE, PHILIPP; Kartellrecht in der anwaltlichen Praxis, 3. Auflage, München 2007.

JERUSALEM, KONRAD; Die Regelung der Mitarbeitergeschäfte im Bankgewerbe durch Compliance, Berlin 1996 .

KAPP, THOMAS; Kartellbehörde durchsucht Geschäftsräume – Was ist zu beachten?, Compliance Report Oktober, Heft 10, 2007, S. 3 – 5.

KAPP, THOMAS; Kartellrecht in der Unternehmenspraxis, Wiesbaden, 2005.

KELLER, DIRK; Außenhaftung des GmbH-Geschäftsführers bei Wettbewerbsverstößen und Verletzung gewerblicher Schutzrechte, GmbHR 2005, S. 1235-1242.

KIETHE, KURT; Vermeidung der Haftung von geschäftsführenden Organen durch Corporate Compliance, GmbHR 2007, S. 393-400

KNOPP, LOTHAR/STEFANIE STRIEGL; Umweltschutzorientierte Betriebsorganisation zur Risikominimierung, BB 1992, S. 2009-2018.

KOCH, HANS-DIETRICH (HRSG.); Der betriebliche Datenschutzbeauftragte, 6. Auflage, Frechen 2006.

KOCK, MARTIN; Einführung einer Ethikrichtlinie im Unternehmen, MDR 2006, S. 673-676.

KORT, MICHAEL; Verhaltensstandardisierung durch Corporate Compliance, NZG 2008, 81-86.

KREKELER, WILHELM/WERNER, ELKE; Unternehmer und Strafrecht, München 2006.

KRIEGER, GERD (HRSG.)/SCHNEIDER, UWE H.(HRSG.); Handbuch Managerhaftung – Risikobereiche und Haftungsfolgen für Vorstand, Geschäftsführer und Aufsichtsrat, Köln 2007.

KUTHE, THORSTEN/RÜCKERT, SUSANNE/SICKINGER, MIRKO; Compliance-Handbuch Kapitalmarktrecht, Heidelberg 2004.

LAMPERT, THOMAS; Gestiegenes Unternehmensrisiko Kartellrecht – Risikoreduzierung durch Competition-Compliance-Programme, BB 2002, S. 2237-2243.

LEISINGER, KLAUS M.; Whistleblowing und Corporate Reputation Management, München 2003.

LENSDORF, LARS; IT-Compliance – Maßnahmen zur Reduzierung von Haftungsrisiken von IT-Verantwortlichen, CR 2007, 413-418.

LENSDORF, LARS/STEEGER, UDO; IT-Compliance im Unternehmen, ITRB 2006, 206-210.

LÖSLER, THOMAS; Spannungen zwischen der Effizienz der internen Compliance und möglichen Reporting-Pflichten des Compliance-Officers, WM 2007, S. 676-683.

LÖSLER, THOMAS; Das moderne Verständnis von Compliance im Finanzmarktrecht, NZG 2005, S. 104-108.
MCVEA, HARRY; Financial Conglomerates and the Chinese Wall, Oxford 1993.
MENGEL, ANJA/HAGEMEISTER, VOLKER; Compliance und arbeitsrechtliche Implementierung im Unternehmen, BB 2007, S. 1386-1392.
MENGEL, ANJA/HAGEMEISTER, VOLKER; Compliance und Arbeitsrecht, BB 2006, S. 2466-2471.
MESSER, HERBERT; Wettbewerbsrechtliche Haftung der Organe juristischer Personen, in: FS Ullmann, 2006, S. 769-779.
MÜLLER, MICHAEL; Whistleblowing – Ein Kündigungsgrund?, NZA 2002, S. 424-437.
OHMANN-SAUER, INGRID; Compliance-Audit im Arbeitsrecht – Handlungsempfehlungen für den Compliance-Beauftragten, AuA 2007, S. 520-524.
PAMPEL, GUNNAR; Die Bedeutung von Compliance-Programmen im Kartellordnungswidrigkeitenrecht, BB 2007, S. 1636-1639.
PELLENS, BERNHARD/HILLEBRANDT, FRANCA/ULMER, BJÖRN; Umsetzung von Corporate-Governance-Richtlinien in der Praxis, BB 2001, S. 1243-1251.
PIRNER, HANS-PETER; Die Organisation von Vertraulichkeit, Frankfurt a.M. 1996.
REITER, CHRISTIAN; Der Schutz des Whistleblowers nach dem Sarbanes-Oxley Act im Rechtsvergleich und im internationalen Arbeitsrecht, RIW 2006, S. 168-178.
RESCH, GERALD/SIDLO, PETER; Emittenten-Compliance im Lichte aktueller nationaler und internationaler Entwicklungen, ÖBA 2005, S. 299-304.
RODEWALD, JÖRG/UNGER, ULRIKE; Corporate Compliance – Organisatorische Vorkehrungen zur Vermeidung von Haftungsfällen der Geschäftsleitung, BB 2006, S. 113-117.
RODEWALD, JÖRG/UNGER, ULRIKE; Kommunikation und Krisenmanagement im Gefüge der Corporate Compliance-Organisation, BB 2007, S. 1629-1634.
ROßNAGEL, ALEXANDER (HRSG.); Handbuch Datenschutzrecht, München 2003.
RUDOLF, INGE; Aufgaben und Stellung des betrieblichen Datenschutzbeauftragten, NZA 1996, 296 – 301.
SCHARPF, MARCUS ALEXANDER; Corporate Governance, Compliance und Chinese Walls, Regensburg 2000.
SCHLICHT, MANUELA; Compliance nach der Umsetzung der MiFID-Richtlinie – Wesentliche Änderungen oder gesetzliche Verankerung schon gelebter Praxis?, BKR 2006, S. 469-475.
SCHNEIDER, UWE H.; Gesellschaftsrechtliche und öffentlich-rechtliche Anforderungen an eine ordnungsgemäße Unternehmensorganisation, DB 1993, S. 1909-1915.
SCHNEIDER, UWE H.; Compliance als Aufgabe der Unternehmensleitung, ZIP 2003, S. 645-650.
SCHNEIDER, UWE H.; Corporate Manslaughter und Corporate Compliance, EuZW 2007, 553.
SCHNEIDER, UWE H.; Die Überlagerung des Konzernrechts durch öffentlich-rechtliche Strukturnormen und Organisationspflichten – Vorüberlegungen zu „Compliance im Konzern“, ZGR 1996, S. 225-246.

SCHNEIDER, UWE H./BUTTLER, JULIA VON; Die Führung von Insider-Verzeichnissen – Neue Compliance-Pflichten für Emittenten, ZIP 2004, S. 1621-1627.

SCHNEIDER, UWE H./SCHNEIDER, SVEN H.; Konzern-Compliance als Aufgabe der Konzernleitung, ZIP 2007, S. 2061-2065.

SCHUMACHER, ANKE; Legal Privilege – auch bei Syndikusanwälten?, in: Compliance Report Heft 10/2007, 12 f.

SCHUSTER, DORIS-MARIA/DARSOW, INGEBJÖRG; Einführung von Ethikrichtlinien durch Direktionsrecht, NZA 2005, S. 273-277.

SCHWEIZER, THILO; Insiderverbote, Interessenkonflikte und Compliance, Berlin 1996.

SETHE, ROLF; Die Verschärfung des insiderrechtlichen Weitergabeverbots, ZBB 2006, S. 243-257.

SIMITIS, SPIROS (HRSG.); Kommentar zum Bundesdatenschutzgesetz, 5. Auflage, Baden-Baden, 2003.

SPINDLER, GERALD; Unternehmensorganisationspflichten, Köln u.a. 2001.

SPINDLER, GERALD/KASTEN, ROMAN A.; Organisationsverpflichtungen nach der MiFID und ihre Umsetzung, AG 2006, S. 785-791.

TINNEFELD, MARIE-THERES/EHMANN, EUGEN/GERLING, RAINER W.; Einführung in das Datenschutzrecht, 4. Auflage, München 2005.

WAGNER, GERHARD; Persönliche Haftung der Unternehmensleitung: die zweite Spur der Produkthaftung?, VersR 2001, S. 1057-1063.

WEBER-REY, DANIELA; Whistleblowing zwischen Corporate Governance und Better Regulation, AG 2006, S. 406-411.

WEICHERT, THILO; Datenschutzstrafrecht – ein zahnloser Tiger?, NStZ 1999, 490 – 496.

WESSING, JÜRGEN; Compliance – Ein Thema auch im Steuerstrafrecht?, SAM 2007, S. 175-181.

WESTIN, ALAN F.; Whistle Blowing! Loyalty and Dissent in the Corporation, New York u.a., 1981.

WISSKIRCHEN, GERLIND/JORDAN, CHRISTOPHER/BISSELS, ALEXANDER; Arbeitsrechtliche Probleme bei der Einführung internationaler Verhaltens- und Ethikrichtlinien (Codes of Conduct/Codes of Ethics), DB 2005, S. 2190-2195.

WOLF, KLAUS; Corporate Compliance – ein neues Schlagwort? Ansatzpunkt zur Umsetzung der Compliance in der Finanzberichterstattung, DStR 2006, S. 1995-2000.

Compliance in der Unternehmerpraxis

Eberhard Vetter

1. Einleitung

Compliance war vor gut zehn Jahren in Deutschland ein noch gänzlich unbekannter Begriff. Er umschreibt die Pflicht, die für das Unternehmen geltenden Gesetze einzuhalten. Dies ist keine neue Erkenntnis. Insoweit ist Compliance zu Recht als eine Binsenweisheit bezeichnet worden.[1] Neu ist jedoch die Einbettung der Compliance in einen größeren Zusammenhang. Es wäre für die Geschäftsleitung eine Illusion zu glauben, Compliance vollziehe sich im Unternehmen stets von selbst. Richtig ist vielmehr, dass eine vorbildliche Compliance sowohl aus organisationstheoretischer Sicht wie auch aus rechtlicher Sicht ein proaktives Vorgehen der Geschäftsleitung erforderlich macht und das gesamte Unternehmen erfassen muss. Compliance beschränkt sich deshalb nicht allein auf das Postulat der Rechtstreue des Unternehmens, sondern umschreibt die Summe der organisatorischen Maßnahmen eines Unternehmens, mit denen gewährleistet werden soll, dass sich die Geschäftsleitung wie auch die Mitarbeiter des Unternehmens rechtmäßig verhalten.

Angesichts des immer umfangreicher werdenden Verantwortungs- und Handlungsrahmens der Geschäftsleitung, der durch zivilrechtliche und öffentlich-rechtliche Pflichten bestimmt wird und aus dem sich eine Vielzahl von rechtlichen Risiken für das Unternehmen ergeben, haben die Vorstände und Geschäftsführer vieler Gesellschaften erkannt, dass sie in weitem Umfang präventiv tätig zu werden haben, wenn sie ihrer Compliance–Verantwortung nachkommen wollen. Sie wollen es gerade nicht allein damit belassen, darauf zu vertrauen, dass sich die Organisation, für die sie Verantwortung tragen, gesetzeskonform und ordnungsgemäß verhält, sondern sie haben Compliance zur Chefsache erklärt. Sie verstehen Compliance nicht nur als bloße Prävention gegenüber Risiken aus Rechtsverstößen, sondern erkennen nicht selten in einem funktionierenden Compliance-Management auch den strategischen Vorteil gegenüber dem Wettbewerb. Dabei ist nicht nur daran zu denken, dass mit Hilfe von Compliance-Maßnahmen vermieden werden kann, dass z. B. ein Unternehmen wegen Rechtsverstößen auf die sog. Schwarze Liste geraten kann und damit von künftigen lukrativen Aufträgen ausgeschlossen ist, sondern auch an die generell wachsende Erkenntnis, dass Unternehmen in

---

1 *Uwe. H. Schneider,* ZIP 2003, 645, 646.

der Regel lieber mit Gesellschaften in Geschäftsbeziehungen treten, bei denen sie nicht mit dem Risiko rechnen müssen, dass dort Rechtsverstöße und Unregelmäßigkeiten festgestellt werden, die auf ihre eigenen Geschäftsaktivitäten und ihre eigene Reputation am Markt durchschlagen können.[2] Damit erweist sich Compliance nicht nur als Bestandteil einer good Corporate Governance sondern auch als Marketing-Faktor.

Die Bedeutung der Compliance darf auch aus volkswirtschaftlicher Sicht nicht unterschätzt werden. Jüngsten Untersuchungen zufolge wird allein in Deutschland der Schaden durch Korruption auf rund 4,3. Milliarden geschätzt.[3] Bemerkenswert ist auch, dass nach einer Umfrage unter Inhouse-Juristen in den USA dem Thema Compliance die oberste Priorität noch vor der Kostenkontrolle eingeräumt wird.[4] Die zunehmende Zahl von Compliance-Beauftragten oder Compliance-Abteilugnen in deutschen Unternehmen bestätigen diesen Befund.

2. Compliance als Geschäftsleitungsaufgabe

2.1 Begriff und Zweck der Compliance

Es gibt weder eine gesetzliche Definition von Compliance, noch ist eine allgemein anerkannte Definition bislang vorhanden. Aber seit der Neufassung des Deutschen Corporate Governance Kodex, die am 20. Juli 2007 im elektronischen Bundesanzeiger bekannt gemacht worden ist,[5] steht eine Umschreibung zur Verfügung, die sich primär an börsennotierte Aktiengesellschaften richtet (§ 161 AktG), die aber durchaus auch als allgemeine Definition der Corporate Compliance gelten kann.[6]

Ziffer 4.1.3 Deutscher Corporate Governance Kodex formuliert wie folgt:

„Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance).“

---

2 Freiwillige ISO-Zertifizierungen und vergleichbare Maßnahmen zur Zertifizierung der Einhaltung von Umwelt und Sozialstandards mögen hier als Vorbilder dienen.

3 Vgl. Studie Wirtschaftskriminalität 2007, herausgegeben von PricewaterhouseCoopers und Martin-Luther-Universität Wittenberg, 2007, S. 15.

4 Umfrage der Association of Corporate Counsel (ACC), Juve Datenbank vom 6. November 2006, im Internet zugänglich über www.juve.de.

5 Im Internet zugänglich unter www.ebundesanzeiger.de

6 Vgl. *Bürkle,* BB 2007, 1797, 1998; *E. Vetter,* DB 2007, 1963.

Hinzuweisen ist darauf, dass die Kodex-Kommission die Pflicht zur Compliance zu Recht nicht nur auf die Beachtung der gesetzlichen Bestimmungen beschränkt hat, sondern auch die unternehmensinternen Regelwerke, also vor allem Satzung und Geschäftsordnung aber z. B. auch Merk- und Informationsblätter, Unterschriftenregelungen, Arbeitsanweisungen und Konzernrundschreiben in die Compliance einbezogen hat.

Handelt es sich um ein Unternehmen, das an der Spitze eines Konzerns steht, erstreckt sich die Compliance auch auf die Konzernunternehmen, soweit das herrschende Unternehmen rechtlich in der Lage ist, die eigenen Compliance-Vorstellungen durchzusetzen.[7] Dies ist kraft Weisungsrecht nach § 308 AktG dann möglich, wenn zwischen dem herrschenden Unternehmen und der Tochtergesellschaft ein Beherrschungsvertrag i. S. von § 291 AktG besteht. Ist die Tochtergesellschaft in der Rechtsform der GmbH organisiert, kann die Weisung auch durch einen entsprechenden Beschluss der Gesellschafterversammlung nach § 37 Abs. 1 GmbHG erfolgen, der für die Geschäftsführer bindend ist.[8] Bei einer Tochtergesellschaft in der Rechtsform der AG bleibt im faktischen Konzern infolge der Schranken der §§ 311 ff. AktG jedoch der Konzernspitze nur die Möglichkeit, gegenüber der Geschäftsleitung der Tochtergesellschaft auf die Beachtung der Compliance-Vorstellungen der Konzernspitze in geeigneter Weise hinzuwirken. Rechtliche Instrumente zur Durchsetzung der Vorstellungen der Konzernspitze bestehen in diesem Fall nicht.[9]

Compliance dient der Risikovorbeugung und der Schadensabwehr im Unternehmen. Sie ist regelmäßig geeignet, Schadensersatzansprüche Dritter gegen die Gesellschaft (sog. Außenhaftung) abzuwehren wie auch Ansprüche der Gesellschaft gegen die Mitglieder des Geschäftsleitungs- und des Aufsichtsorgans (sog. Innenhaftung) zu vermeiden. Dabei ist von erheblicher Bedeutung, dass im Bereich der Innenhaftung die Mitglieder des Vorstands einer AG die Beweislast dafür tragen, dass sie bei ihrer Geschäftsführung die notwendige Sorgfalt beachtet haben (§ 93 Abs. 2 Satz 2 AktG). Im GmbHG findet sich keine mit § 93 Abs. 2 AktG vergleichbare Vorschrift. Für die Geschäftsführer einer GmbH gilt nach allgemeiner Meinung gleichwohl die Regelung des § 93 Abs. 2 Satz 2 AktG analog.[10]

Compliance versteht sich auch als Teil des Risikofrüherkennungs- und Überwachungssystem (sog. Risikomanagement), zu dessen Einrichtung und Unterhaltung der Vorstand einer AG nach § 91 Abs. 2 AktG im Hinblick auf existenzgefährdende Risiken verpflichtet ist und wie es auch in Ziffer 4.1.4 Deutscher Corporate Governance Kodex ausdrücklich angesprochen wird. Zahlreiche Risiken aus Rechtsverstößen können durchaus eine bestandsgefährende Dimension einnehmen, was die Nähe der Compliance zum Risikofrüherkennungssystem im Sinne § 91 Abs. 2 AktG unterstreicht.[11] Das GmbHG enthält keine mit § 91 Abs. 2 AktG vergleichbare Vorschrift. Gleichwohl besteht allgemein Einigkeit, dass auch die Geschäfts-

7 *Fleischer,* DB 2005, 759, 763; vgl. auch *Sven H. Schneider/Uwe H. Schneider,* AG 2005, 57, 59.

8 *Altmeppen,* in: Roth/Altmeppen, GmbHG, 5. Aufl. 2005, § 37 Rn. 3; *Zöllner/Noack,* in: Baumbach/Hueck, GmbHG, 18. Aufl. 2006, § 37 Rn. 18.

9 Vgl. generell zur Konzern-Compliance *Uwe H. Schneider/Sven H. Schneider,* ZIP 2007, 2061.

10 BGH v. 4. 11. 2002 – II ZR 224/00, BGHZ 152, 280, 283; *Zöllner/Noack,* in: Baumbach/Hueck, GmbHG, 18. Aufl. 2006, § 43 Rn. 204.

11 Ähnlich *Uwe H. Schneider,* ZIP 2003, 645, 649.

führung einer GmbH eine entsprechende Pflicht und systematische Maßnahmen zur Erfassung bestandsgefährdender Risiken zu ergreifen hat, sofern das Unternehmen eine kritische Größe erreicht hat.[12] Entsprechendes lässt sich auf die Compliance-Verantwortung übertragen. Compliance versteht sich primär als Prävention reicht aber darüber hinaus. Auch eine vorbildliche Compliance-Organisation vermag Regelverstöße nicht vollkommen auszuschließen. Compliance umfasst deshalb auch das Krisenmangement im Unternehmen. Bei Eintritt einer Krise durch einen Regelverstoß findet die Compliance Ausdruck in den Maßnahmen zur Krisenbewältigung und Schadensminderung.[13]

2.2 Rechtsgrundlage der Compliance

Das Deutsche Recht kennt keine Gesetzesnorm, die die Geschäftsleitung einer AG oder GmbH ausdrücklich zur Vornahme systematischer Compliance-Maßnahmen und zur Einrichtung einer allgemeinen Compliance-Organisation verpflichtet. Allerdings sieht § 76 Abs. 1 AktG vor, dass der Vorstand die Gesellschaft unter eigener Verantwortung zu leiten hat und, wie § 93 Abs. 1 AktG bestimmt, dabei die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden hat. Für die GmbH Geschäftsführer findet sich, was ihre Sorgfaltspflichten anbetrifft, die Parallele zu § 93 Abs. 1 AktG in § 43 Abs. 1 GmbHG. Aus den §§ 76 Abs. 1 und 93 Abs. 1 AktG lässt sich grundsätzlich eine organschaftliche Pflicht des Vorstands zur Compliance ableiten.[14] Als weitere Rechtsgrundlage für die Ergreifung von Compliance-Maßnahmen lassen sich auch die §§ 3, 9 und 130 OWiG heranziehen. § 130 OWiG weist die Pflichtenstellung der Aktiengesellschaft als Inhaberin des Betriebes bzw. des Unternehmens dem Vorstand, beziehungsweise der Geschäftsführung der juristischen Person zu mit der Folge, dass das Organmitglied grundsätzlich für alle Verletzungen bußgeldbewehrter Pflichten in einem Unternehmen zur Rechenschaft gezogen werden kann, soweit der Verstoß auf eine Verletzung von Aufsichtspflichten zurückgeführt werden kann. Berücksichtigt man, dass eine Vielzahl öffentlich-rechtlicher Pflichten eines Unternehmens in irgendeiner Form mit einem Bußgeld bewehrt sind (z. B. Kartellrecht, Kapitalmarktrecht, Umweltrecht, Datenschutzrecht, Arbeitsstrafrecht, Außenwirtschaftsrecht), lässt sich dem Ordnungswidrigkeitenrecht damit mittelbar die Verpflichtung zur Einrichtung einer Compliance-Organisation entnehmen, für die die Mitglieder des Geschäftsleitungsorgans selbst verantwortlich sind.[15]

---

12 *Altmeppen,* in: Roth/Altmeppen, GmbHG, 5. Aufl. 2005, § 43 Rn. 10; Lutter/Hommelhoff/*Kleindiek,* GmbHG, 16. Aufl. 2005, § 43 Rn. 11.

13 Vgl. dazu z. B. *Rodewald/Unger,* BB 2007, 1629, 1633.

14 *Fleischer,* AG 2003, 291, 299; *Uwe. H. Schneider,* ZIP 2003, 645, 648; *E. Vetter,* in: Krieger/Uwe H. Schneider (Hrsg.), Handbuch Managerhaftung, 2007, § 17 Rn. 29; zurückhaltend freilich *Hauschka,* ZIP 2004, 877, 882.

15 Siehe zur Kartellrechts-Compliance Kapitel 10: Janssen, Kartellrechts-Compliance und weiter z. B. *Dreher,* in: Krieger/Uwe. H. Schneider (Hrsg.), Managerhaftung, 2007, § 29 Rn. 59 ff.; *Pampel,* BB 2007, 1636; zur Kapitalmarktrechts-Compliance z. B. *Krämer,* in: Krieger/Uwe. H. Schneider (Hrsg.), Managerhaftung, 2007, § 26 Rn. 67 ff. und zur Umweltrechts-Compliance z. B. *Uwer,* in: Krieger/Uwe. H. Schneider (Hrsg.), Managerhaftung, 2007, § 32 Rn. 18 ff.

Die Veranwortung für die Einrichtung eines Compliance-Systems trägt die Geschäftsleitung im Rahmen ihrer Leitungsaufgabe.[16] Eine Verpflichtung für konkrete Compliance-Maßnahmen in einem Unternehmen lässt sich aus den genannten Vorschriften jedoch nicht ableiten. Auch der Deutsche Corporate Governance Kodex enthält keine konkreten Vorgaben oder Empfehlungen zu Art und Umfang der Compliance. Compliance ist keine konfektionierte Standard-Organisation. Vielmehr hängt die konkrete Ausgestaltung der Compliance in einem Untenehmen vom jeweiligen Geschäftszweig und dem konkreten Unternehmensgegenstand, der Größe und Komplexität des Unternehmens und der Unternehmensstruktur und damit letztlich von seinem individuellen Risikoprofil ab.[17] Die individuellen Compliance-Maßnahmen stehen im Übrigen generell unter dem Vorbehalt des unternehmerischen Ermessens des Vorstands im Sinne von § 93 Abs. 1 S 2 AktG und unterliegen damit der sog. Business Judgment Rule. Der Vorstand hat über Art und Umfang der organisatorischen Maßnahmen zu entscheiden, wie für die Rechtstreue im Unternehmen gesorgt werden soll und auf welche Weise Rechtsverstöße verhindert werden sollen. Dies bedeutet, dass das Geschäftsleitungsorgan bei der Festlegung der Anforderungen und der Dimensionierung einer Compliance-Organisation nach sorgfältiger Ermittlung der relevanten Risikofaktoren das individuelle Gefahrenpotential und Risikoszenario des Unternehmens beurteilen und bewerten muss. Die Geschäftsleitung muss die jeweiligen Konsequenzen für das Unternehmen vor Augen haben, die bei Eintritt eines spezifischen Risikos entstehen können. Versäumnisse können einen Sorgfaltsverstoß im Sinne von § 93 Abs. 2 AktG und § 43 Abs. Abs. 2 GmbHG bilden.[18]

2.3 Das Risikopotential der Unternehmen bei Rechtsverstößen

Die Risiken der Unternehmen aus Gesetzesverstößen, Schadensfällen oder sonstigen Missständen infolge von unterlassener oder unzureichender Compliance-Maßnahmen sind vielfältig und sollten keinesfalls unterschätzt werden. Jüngste Negativbeispiele, die in der Öffentlichkeit große Aufmerksamkeit erzielt haben, können dabei als Mahnung dafür dienen (VW, Siemens, Ahold, WestLB), welche Wirkungen das Bekanntwerden von Gesetzesverstößen auf das öffentliche Ansehen eines Unternehmens, die Motivation seiner Mitarbeiter, die Akzeptanz seiner Produkte am Markt und damit letztlich auf seine wirtschaftliche Situation haben kann.

Ein Rechtsverstoß und Compliance-bezogener Missstand im Unternehmen kann dramatische Konsequenzen für das Unternehmen bedeuten, die vom Reputationsverlust über erhebliche

---

16 *Bürkle,* in: Hauschka (Hrsg.), Corporate Compliance, 2007, § 8 Rn. 5; *Fleischer,* in: Fleischer (Hrsg.), Handbuch des Vorstandsrechts, 2006, § 8 Rn. 44; *Uwe. H. Schneider,* ZIP 2003, 645, 646.

17 Siehe allgemein *Fleischer,* in: Fleischer (Hrsg.), Handbuch des Vorstandsrechts, 2006, § 8 Rn. 44; *Hauschka,* AG 2004, 461, 465; *Hefermehl/Spindler,* in: MüKo/AktG, 2. Aufl. 2004, § 76 Rn. 28.

18 *Fleischer,* AG 2003, 291, 300.

finanzielle Einbußen bis hin zu strafrechtlichen Maßnahmen reichen. Beispielhaft lassen sich die folgenden Konsequenzen zu nennen:

- Gefährdung durch negative Presseberichte über das Unternehmen
- Werteverfall für die Shareholder
- Eingreifen des Aufsichtsrates
- Eingreifen von Aufsichtsbehörden
- Betriebsstillegung
- Unternehmenskrise, Gefährdung der Arbeitsplätze
- Bußgelder bis zu 10 % des Konzernumsatzes, Vergabesperre und „Blacklisting“
- Verfall des mit inkriminierten Geschäften erzielten Erlöses an die Staatskasse
- Untersuchungshaft und Haft für Manager, Geldstrafen für Management und Unternehmen
- Einstweilige Verfügung gegen einzelne Geschäftsaktivitäten
- Pfändung von Bankkonten
- Schadensersatzforderungen durch Kunden, Wettbewerber und Verbraucher
- Beschäftigung des Managements mit Verteidigungsaktivitäten zu Lasten der Konzentration auf das Geschäft
- Bedrohung der beruflichen Existenz der Organmitglieder

3. Compliance als Aufgabe des Aufsichtsrats

Ziffer 3.4 Abs. 2 Deutscher Corporate Governance Kodex in der Fassung vom 20. Juli 2007 geht auf die Berichtspflichten des Vorstands gegenüber dem Aufsichtsrat nach § 90 AktG ein und ergänzt sie ausdrücklich um Informationen zur Compliance im Unternehmen. Aus Ziffer 3.4 Abs. 2 wie auch aus Ziffer 5.3.2 Deutscher Corporate Governance Kodex wird damit deutlich, dass Compliance auch im Verantwortungsbereich des Aufsichtsrats liegt, der im Rahmen seiner allgemeinen Überwachungsaufgabe nach § 111 Abs. 1 AktG die Rechtmäßigkeit und Ordnungsmäßigkeit der Geschäftsleitung des Vorstands zu kontrollieren hat.[19] Dies schließt die Verantwortung des Aufsichtsrats ein, den Vorstand dahin zu überwachen, ob er

---

19 *E. Vetter,* in: Marsch-Barner/Schäfer (Hrsg.), Handbuch börsennotierte AG, 2005, § 26 Rn. 10; *Wiesner,* in: Hoffmann-Becking (Hrsg.), Münchener Handbuch Gesellschaftsrecht AG, 3. Aufl. 2007, § 25 Rn. 5.

der Compliance-Verantwortung nachgekommen und bei seiner Entscheidung über Präventions-und Kontrollmaßnahmen wie auch bei der Auswahl und dem Aufbau von Sicherungseinrichtungen von seinem unternehmerischen Ermessen pflichtgemäß Gebrauch gemacht hat. Insoweit besteht auch eine enge Beziehung zur Kontrolle des Systems zur Erfassung bestandsgefährdender Risiken im Sinne von § 91 Abs. 2 AktG.[20]

Die Überwachung dieser wichtigen Vorstandsverantwortung durch den Aufsichtsrat soll nach der jüngsten Ergänzung in Ziff. 5.3.2 Satz 1 Deutscher Corporate Governance Kodex vorrangig vom Prüfungsausschuss (Audit Committee) wahrgenommen werden, dessen Einrichtung nach Art. 41 der Prüferrichtlinie für börsennotierte Unternehmen besondere Bedeutung erhält.[21]

4. Die Bandbreite Compliance – relevanter Rechtsgebiete

Die Risikoanalyse der Unternehmensleitung muss auf die konkrete Unternehmenssituation ausgerichtet werden. Dies gilt insbesondere für die von einem Unternehmen zu beachtenden Rechtsregeln, die naturgemäß von vielen Faktoren bestimmt werden, vor allem von seiner Rechtsform, Organisation, Größe und Komplexität wie auch dem speziellen Wirtschafszweig, in dem es tätig ist. Typischerweise handelt es sich bei den relevanten Compliance-Bereichen um ein ganzes Bündel von Rechtsgebieten, für deren Beachtung die Geschäftsleitung Verantwortung trägt.

---

20 *E. Vetter,* DB 2007, 1963, 1966.

21 Richtline 2006/43/EG des Europäischen Parlaments und des Rates vom 17.5.2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinie 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates. Siehe auch den Referentenentwurf des Bilanzrechtsmodernisierungsgesetzes (BilMoG) und dazu: *Ernst/Seidler*, BB 2007, 2557, 2564.

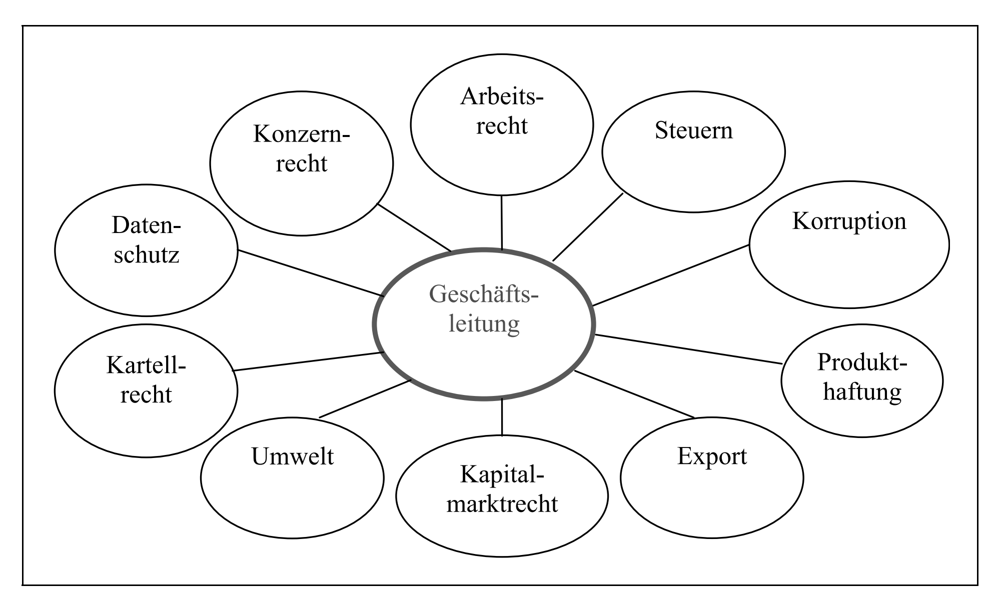


Abbildung 1: *Compliance-relevante Rechtsgebiete*[22]

5. Fünf Elemente der Compliance

Compliance versteht sich als aktive Risikovorbeugung im Unternehmen. Neben vielen einzelnen organisatorischen Maßnahmen, die ein effizientes Compliance-Management voraussetzt, verlangt sie eine Compliance-Kultur, die im Unternehmen breit verankert ist und von Geschäftsleitung und Belegschaft auch tatsächlich gelebt wird. Für die Einrichtung einer Compliance-Organisation bedarf es bestimmter organisatorischer Maßnahmen im Rahmen einer strukturierten Vorgehensweise, die sich in fünf Schritten wie folgt gliedern lässt:[23]

---

22 Abb. in Anlehnung an *Hauschka*: Präsentation Compliance in der Unternehmenspraxis, LBBW-Forum Stuttgart vom 28. Juni 2007.

23 Anders z. B. *Hauschka,* in: Hauschka (Hrsg.), Corporate Compliance, 2007, § 1 Rn. 33, der ein dreistufiges Modell beschreibt; siehe auch *Hauschka,* DB 2006, 1143.

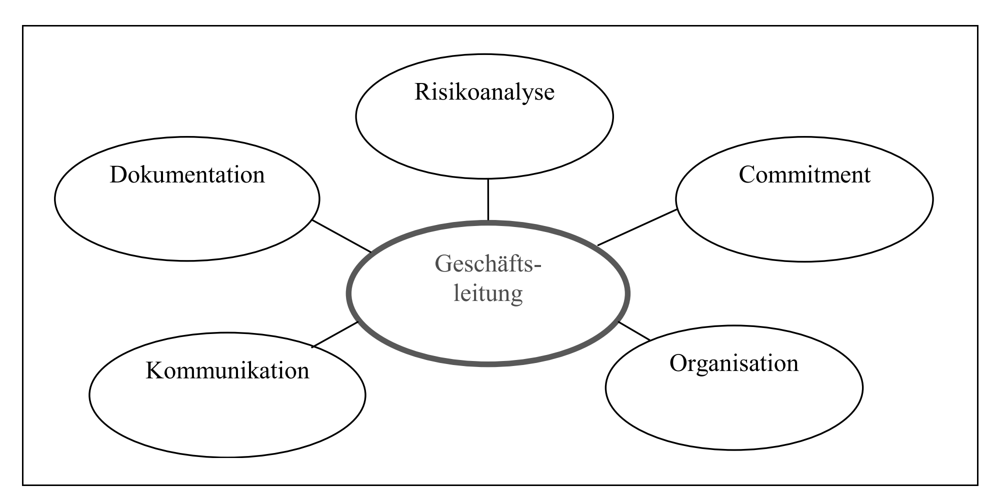


Abbildung 2: *Elemente der Compliance.*[24]

5.1 Risikoanalyse

Erster Schritt der Absicherung gegen Rechtsrisiken ist die Identifikation der im jeweiligen Unternehmen vorhandenen Rechtsrisiken, die Abschätzung des Schadensumfangs bei Eintritt des einzelnen Risikos nach sachlicher und monetärer Größe sowie die Abschätzung der jeweiligen Eintrittswahrscheinlichkeit eines Rechtsverstoßes und der daraus abzuleitenden Schritte zur Risikovorbeugung.

Als konkretes Beispiel der Risikoanalyse soll das Korruptionsproblem dienen.[25] Zur Erkennung von Korruptionsrisiken im Unternehmen kann z. B. der Katalog herangezogen werden, der bei steuerlichen Betriebsprüfungen der Oberfinanzdirektion Düsseldorf zur Anwendung kommt.[26] Er ist nicht nur geeignet, im Unternehmen daraus eigene Präventionsmaßnahmen im Bereich der Korruptionsbekämpfung zu entwickeln, sondern kann auch als generelles Muster für einen unternehmensspezifischen Prüfkatalog in anderen Compliance-relevanten Bereichen dienen.

---

24 Abb. von *Hauschka*: Präsentation Compliance in der Unternehmenspraxis, LBBW-Forum Stuttgart vom 28. Juni 2007.

25 Vgl. dazu z. B. *Hauschka/Greve,* BB 2007, 165.

26 Leitfaden der Oberfinanzdirektion Düsseldorf. Die Behandlung von Vorteilszuwendungen im Sinne des § 4 Abs. 5 S. 1 Nr. 10 EStG, 2002.

Der Katalog der Oberfinanzdirektion Düsseldorf führt die folgenden Gesichtspunkte auf:

- Verbuchung ohne Empfängerbenennung oder nicht existierender Empfänger;
- keine schriftliche Vereinbarung mit dem Empfänger;
- Bankkonto des Geldempfängers ist Nummernkonto;
- Konten an Off-Shore-Plätzen (z. B. Bahamas, Bermuda, Cayman lslands Libanon, Liechtenstein, Schweiz);
- Zahlungen an Vermittler, Makler, Provisionen, Erfolgshonorare;
- Geldempfänger ist eine „Briefkastenfirma";
- Barzahlungsvorgänge;
- Speisung „schwarzer Kassen";
- fingierte Leistungsinhalte und Überfakturierungen.

5.2 Commitment

Die Erfahrungen der Unternehmenspraxis aber auch die in der Öffentlichkeit bekannt gewordenen Fälle von groben Missständen führen zu der Erkenntnis, dass die Compliance-Organisation steht und fällt mit dem Bekenntnis der Unternehmensspitze zur Compliance im Unternehmen. Compliance darf kein Formalakt und keine bloße Pflichtübung sein. Die Unternehmensleitung muss sich vielmehr uneingeschränkt der Sache verpflichtet fühlen und Compliance als Chefsache behandeln. Sie muss das Thema Compliance proaktiv angehen und klare Botschaften an die Mitarbeiter senden und deutlich machen, dass Rechtsverstöße im Unternehmen von der Geschäftsleitung nicht geduldet werden und bei Verstößen entsprechende Sanktionen ergriffen werden.[27] Dies schließt zwingend das unmissverständliche Signal der Geschäftsleitung an die Belegschaft ein, dass ein Geschäftsabschluss unter Missachtung der im Unternehmen geltenden Compliance-Grundsätze keinesfalls dem Unternehmensinteresse dient, sondern Geschäfte, die unter Verstoß gegen Rechtsvorschriften zustande kommen, dem Unternehmen schaden.

---

27 Vgl. zur sog. Zero Tolerance Policy *Uwe H. Schneider,* ZIP 2003, 645, 649 einerseits und *Hauschka,* ZIP 2004, 877, 882 andererseits.

5.3 Kommunikation

Das Commitment der Geschäftsleitung und die Botschaft, dass sich das Unternehmen an die maßgeblichen Rechtsvorschriften wie auch an die internen Vorschriften und Regularien halten will und dazu entsprechende Maßnahmen zur Prävention und Kontrolle getroffen hat, muss in geeigneter Weise sowohl im Unternehmen aber auch an Geschäftspartner kommuniziert werden. Hierfür bieten sich aus praktischer Sicht verschiedene Instrumente an:

- Mission Statement“ der Geschäftsleitung
- Internet-Homepage des Unternehmens
- Intranet-Seiten zu Compliance-Themen, E-Mails der Geschäftsleitung an die Mitarbeiter
- Informationsbroschüren, Richtlinien
- Schulungen und Veranstaltungen mit externen Trainern und Beratern
- Präsentationen des Korruptions-, Umwelt-, etc.-, Beauftragten
- Tagungen der Vertriebs- oder Niederlassungsleiter zu Compliance-Themen
- Informationstermine bei Umwelt-, Sicherheitsbeauftragten etc.
- Besprechung der internen Dokumentation für den „Schadensfall“
- „e-Schulungen“ im Kartellrecht, Datenschutz, Arbeitsrecht (AGG), in der Korruptionsbekämpfung etc.[28]

Kommunikation setzt schließlich auch voraus, dass die im Unternehmen bestehenden Rechtsrisken in den jeweiligen Hierarchieebenen kommuniziert werden, damit von den entsprechenden Stellen im Unternehmen auch die zur Risikobeherrschung notwendigen Maßnahmen ergriffen werden können.[29]

5.4 Organisation

Compliance setzt eine klare Organisationsstruktur im Unternehmen voraus. Sie erfasst zuerst das Geschäftsleitungsorgan, für das kraft Gesetzes das Prinzip der Gesamtzuständigkeit und Gesamtverantwortung gilt. Die moderne Unternehmenspraxis erzwingt hier bei einem mehr-

---

28 Vgl. z. B. www.interactive-dialogues.com.

29 Siehe dazu z. B. LG München I v. 5. 4. 2007 – 5HK O 15964/06, AG 2007, 417 zum Risikofrüherkennungssystem.

köpfigen Geschäftleitungsorgan regelmäßig Modifikationen, um den vielfältigen Anforderungen und der Komplexität der Leitungsaufgabe angemessen Rechnung zu tragen. Richtiger Ort für solche Regelungen ist die Geschäftsordnung, in der auch die Ressortzuständigkeiten der einzelnen Mitglieder der Geschäftsleitung sowie die dem Gesamtorgan vorbehaltenen Angelegenheiten und die dabei notwendigen Beschlussmehrheiten geregelt werden sollten. Fehlen entsprechende Regelungen zur Beschlussfassung, gilt kraft Gesetzes das Prinzip der Einstimmigkeit[30] und der Gesamtgeschäftsführung, was in der modernen Unternehmenspraxis kaum mit einer praktikablen und effizienten Wahrnehmung der Leitungsaufgabe vereinbar ist. In einem mehrköpfigen Geschäftleitungsorgan wird man derartige Regelungen deshalb zu den Voraussetzungen einer guten Corporate Governance zu zählen haben. Dies bestätigt auch Ziff. 4. 2.1 Satz 2 Deutscher Corporate Governance Kodex in der am 20. Juli 2007 bekannt gemachten Fassung, die ausdrücklich den Erlass entsprechender Regelungen empfiehlt.[31]

Die Geschäftsverteilung in der Geschäftleitung durch Einrichtung spezieller Ressorts führt zwangsläufig zu einer gespaltenen Pflichtenstellung des einzelnen Geschäftleitungsmitglieds.[32] Im eigenen Ressort übernimmt das Mitglied eine leitende und verwaltende Tätigkeit. Hinsichtlich der Ressorts der anderen Mitglieder hat es eine beaufsichtigende Funktion. Von der Ressortbildung und Einzelgeschäftsführung unberührt bleiben die Aufgaben, die dem Geschäftleitungsorgan kraft Gesetzes zwingend als Gesamtaufgabe zugewiesen sind und die als originäre Führungsfunktionen zu qualifizieren sind.[33] Hierzu zählt auch die Verantwortung für die Einrichtung einer dem Risikoprofil des Unternehmens angemessenen Corporate Compliance-Organisation als Präventionsmaßnahme.[34] Dies schließt z. B. die Einsetzung eines Compliance-Beauftragten im Unternehmen[35] oder die Einrichtung einer Compliance-Abteilung ein.

Neben der horizontalen Aufteilung von Aufgaben und Verantwortung innerhalb des Geschäftleitungsorgans durch die Begründung von Ressortzuständigkeiten besteht die Möglichkeit der vertikalen Delegation auf nachgeordnete Hierarchieebenen, soweit nicht originäre Führungsfunktionen verlagert werden sollen oder gesetzliche Schranken einer Delegation entgegenstehen. Im weiteren Sinne der Delegation ist darunter auch das Outsourcing auf externe Dritte zu verstehen.

---

30 *Kort,* in: Großkommentar AktG, 4. Aufl. 2006, § 77 Rn. 6 und 10; *Wiesner,* in: Hoffmann-Becking (Hrsg.), Münchener Handbuch Gesellschaftsrecht AG, 3. Aufl. 2007, § 22 Rn. 6; *Zöllner/Noack,* in: Baumbach/Hueck, GmbHG, 18. Aufl. 2006, § 37 Rn. 24.

31 Siehe dazu *E. Vetter,* DB 2007, 1963, 1964.

32 *Fleischer,* NZG 2003, 449, 452; *Hefermehl/Spindler,* in: MüKo/AktG, 2. Aufl. 2004, § 77 Rn. 28; *Zöllner/Noack,* in: Baumbach/Hueck, GmbHG, 18. Aufl. 2006, § 37 Rn. 27; *E. Vetter,* in: Krieger/Uwe H. Schneider (Hrsg.), Handbuch Managerhaftung, 2007, § 17 Rn. 19.

33 *Hoffmann-Becking,* ZGR 1998, 497, 508; *Hüffer,* AktG, 7. Aufl. 2005 § 76 Rn. 8; *Zöllner/Noack,* in: Baumbach/Hueck, GmbHG, 18. Aufl. 2006, § 35 Rn. 33.; siehe auch OLG Düsseldorf v. 15. 11. 1984 – 8 U 22/84, ZIP 1984, 1476, 1478.

34 Vgl. dazu z. B. *Hauschka*, NJW 20004, 257, 259; *Hefermehl/Spindler,* in: MüKo/AktG, 2. Aufl. 2004, § 76 Rn. 17; *Rodewald/Unger,* BB 2006, 113; *Uwe H. Schneider,* ZIP 2003, 645, 647.

35 Vgl. z. B. *Bürkle,* in: Hauschka (Hrsg.), Corporate Compliance, 2007, § 2 Rn. 11 ff.

Aus formaler Sicht gilt sowohl für die Organisation innerhalb des Geschäftsleitungsorgans wie auch für die Delegation auf nachgeordnete Unternehmensebenen, dass die jeweiligen Zuständigkeiten unmissverständlich festgelegt und die Funktionen und Maßnahmen klar und eindeutig definiert sein müssen. Dabei ist sicherzustellen, dass die verschiedenen Verantwortungsbereiche überschneidungsfrei sind. Es versteht sich von selbst, dass die Organisations- und Delegationsentscheidungen ebenso wie die Berichtswege und Kompetenzen schriftlich niedergelegt werden müssen, damit die Entscheidungen im Unternehmen kommuniziert und jederzeit nachvollziehbar und nachprüfbar sind.[36]

In inhaltlicher Hinsicht muss bei der Organisation und Delegation von Aufgaben und Verantwortlichkeiten beachtet werden, dass die Personalauswahl sorgfältig erfolgt, eine gründliche Einweisung der Person in die neue Aufgabe stattfindet und auch eine regelmäßige Überwachung der ordnungsgemäßen Wahrnehmung der übernommenen Aufgabe erfolgt.[37]

Die Organisation erstreckt sich auch auf systematische und verfahrensmäßige Vorkehrungen im Unternehmen zur Einrichtung einer Informations- und Kommunikationsorganisation, die gewährleisten sollen, dass die unternehmerischen Entscheidungen der Geschäftsleitung den Kriterien der Verfahrenskontrolle im Sinne von § 93 Abs. 1 Satz 2 AktG genügen und bei der Anwendung des unternehmerischen Ermessens[38] die Informationen der Geschäftsleitung als Entscheidungsgrundlage auch zur Verfügung stehen.[39]

5.5 Dokumentation

Es versteht sich fast von selbst, dass ein Unternehmen nur dann als ordentlich geführt bezeichnet werden kann und über eine effiziente Compliance verfügt, wenn diese Tatsache auch belegt werden kann. Damit ist der letzte Baustein der Compliance angesprochen, nämlich die Dokumentation der Entscheidungen, Prozesse, Maßnahmen und Berichtswege.

---

36 Siehe dazu z. B. LG München I v. 5. 4. 2007 – 5HK O 15964/06, AG 2007, 417 zum Risikofrüherkennungssystem.

37 Vgl. z. B. *Schmidt-Husson,* in: Hauschka (Hrsg.), Corporate Compliance, 2007, § 7 Rn. 21 ff.; Rn. 33; *E. Vetter,* in: Krieger/Uwe H. Schneider (Hrsg.), Handbuch Managerhaftung, 2007, § 17 Rn. 63 und 68.

38 Vgl. dazu auch die Regeln des Arbeitskreises“ Externe und interne Überwachung der Unternehmung“ der Schmalenbach Gesellschaft für Betreibswirtschaft e. V., ZIP 2006, 1068.

39 Vgl. dazu z. B. *Buck-Heeb,* in: Hauschka (Hrsg.), Corporate Compliance, 2007, § 2 Rn. 15 ff.; siehe auch *Kinzl,* DB 2004, 1653, 1654.

Die Geschäftsordnung des Vorstands bzw. der Geschäftsführung bedarf der Schriftform.[40] Dabei ist darauf zu achten, dass die Geschäftsordnung von dem nach Gesetz oder Satzung festgelegten Gremium erlassen wird. Auch die Ressortverteilung bedarf der Schriftform. Wie die Unternehmenspraxis zeigt, ist dies nicht immer der Fall. Vielfach ist festzustellen, dass entweder eine Aufgabenverteilung in schriftlicher Form nicht vorhanden ist oder aber die im Unternehmen geltende Ressortverteilung längst nicht mehr den tatsächlichen Gegebenheiten entspricht und die für die Festlegung der Ressorts zuständigen Organe und Gremien hierüber nicht informiert sind.

Die Beratungen und Entscheidungen des Geschäftsleitungsorgans finden im Regelfall in entsprechenden Sitzungen statt und müssen in ausreichender Form protokolliert werden. Gleiches gilt für Entscheidungen, die auf telefonischem Wege gefasst worden sind. Schulungen von Mitarbeitern müssen ebenso schriftlich festgehalten werden, wie Kontrollroutinen, Prüfungen und Tests.

Nur wenn die im Unternehmen durchgeführten Compliance-Maßnahmen ausreichend dokumentiert sind und entsprechende Nachweise z. B. im Fall eines Regelverstoßes oder eines Unfalls einer im Übrigen ernsthaft betriebenen und sonst funktionierenden Compliance vorgelegt werden können, besteht die berechtigte Hoffnung, dass Schadensersatzansprüche Dritter gegen das Unternehmen oder die Mitglieder der Geschäftsleitung sowie sonstige Sanktionen gegen Unternehmen, die Mitglieder der Geschäftsleitung oder andere handelnde Personen erfolgreich abgewendet oder abgemildert werden können.

---

40 BFH v. 26. 4. 1984 – V R 128/79, BFHE 141, 433, 447; OLG Koblenz v. 9. 6. 1998 – 3 U 1662/89, 953, 954; *Dreher,* ZGR 1992, 22, 59; *Hüffer,* AktG, 7. Aufl. 2006, § 77 Rn. 21; *E. Vetter,* in: Krieger/Uwe H. Schneider (Hrsg.), Handbuch Managerhaftung, 2007, § 17 Rn. 31 und 32.

Pflichten der Geschäftsleitung & Aufbau einer Compliance Organisation

Gregor Wecker / Stefan Galla

Zusammenfassung

Aufgrund der unterschiedlichen Anforderungen, die an Unternehmen vom Gesetzgeber gestellt werden, kann es keinen allgemeingültigen Compliance Begriff geben. Vielmehr variieren die Anforderungen individuell bei jedem Unternehmen. Entsprechend kann man in der täglichen Beratungspraxis feststellen, wie unterschiedlich das Thema Compliance angegangen wird. Während Banken und Versicherungen aufgrund der hohen Regulierungsdichte in diesem Geschäftsbereich längst eine diversifizierte Compliance Struktur – meist mit Compliance Officer – eingeführt haben und das Thema unternehmensintern einen hohen Stellenwert hat, kennt man den Begriff Compliance in kleinen und mittelständischen Unternehmen teilweise nur vom Hörensagen. Das soll natürlich nicht bedeuten, dass sich solche Unternehmen nicht bemühen die für sie geltenden Vorschriften einzuhalten.

In vielen Unternehmen wird mittlerweile versucht das Thema „Aufbau einer Compliance Organisation" strukturiert anzugehen. Für die Umsetzung bieten sich vielgestaltige IT-Programme an. Über solche Programme können u. a. Schulungen (eLearning), z. B. hinsichtlich des Inhalts von Handbüchern, gezielt für spezielle Mitarbeitergruppen durchgeführt werden. Heutige IT-Programme bieten jedoch darüber hinaus vielschichtige Möglichkeiten die Compliance-Struktur in einem Unternehmen zu verbessern. Über Beteiligungsmanagement- und Vertragsverwaltungssysteme können Datenbanken aufgebaut werden, die über das Internet weltweit von Führungskräften des Unternehmens genutzt werden können. Die bei richtiger Anwendung hierdurch entstehende Datengenauigkeit ist sicherlich ein wichtiger Baustein in einer Compliance-Struktur eines weltweit vernetzten Konzerns. Jedoch nicht nur große – weltweit operierende – Unternehmen profitieren von einer guten Compliance-Struktur. Auch auf kleine und mittelständische Unternehmen sind viele Bausteine einer solchen Compliance-Struktur übertragbar.

Aber auch die beste IT-Infrastruktur, Schulungen und Handbücher sowie die Schaffung einer Personalstruktur mit genau definierten Überwachungspflichten nutzen nur dann wirklich, wenn die Mitarbeiter für das Thema Compliance gewonnen werden können und dieses Thema nicht als Behinderung ihrer täglichen Arbeit betrachten.

Nachfolgend sollen zunächst einige Begrifflichkeiten geklärt werden, bevor die These überprüft wird, ob eine Pflicht der Geschäftsleitung zur Errichtung einer Compliance Organisation besteht und auf verschiedene Möglichkeiten zur Errichtung einer Compliance-Struktur eingegangen wird. Hierbei wird auch thematisiert, inwieweit sich aus dem Gesetz bzw. aus der Rechtsprechung die Pflicht zur Einrichtung einer internen Revision als Teil einer Compliance-Organisation bzw. die Pflicht zur effizienten Informationsorganisation ergibt.

1. Corporate Compliance – Begriffsdefinition und -abgrenzung

Der Begriff Compliance ist ein Oberbegriff, und bedeutet

- Einhaltung sämtlicher für das jeweilige Unternehmen relevanten gesetzlichen Pflichten, Vorschriften, Regeln,
- fachliche Kompetenz und persönliche Verantwortung im Umgang mit externen Regeln, internen Regeln und Vorgaben der Gesellschafter und Vertragspartner sowie
- Einhaltung von Vorgaben der Zentrale durch Konzerneinheiten.

Seit der letzten Überarbeitung des Deutschen Corporate Governance Kodex (DCGK) vom 14. Juni 2007 wird der Begriff Compliance in Ziffer 4.1.3 DCGK zudem wie folgt legal definiert:

> *„Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen* ***und der unternehmensinternen Richtlinien*** *zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin* ***(Compliance)****.“*

Der Begriff ist zur Klarstellung zunächst abzugrenzen von weiteren Begriffen, die häufig mit dem Begriff Corporate Compliance verwechselt werden.

- Der Begriff **Corporate Governance** umfasst beispielsweise als weiterer Begriff alle gesetzlichen Regeln und anerkannten Standards sorgfältiger Unternehmensführung.
- Bei **Risk Management Systemen** i.S.d. § 91 Abs. 2 AktG handelt es sich um die Einrichtung von Früherkennungs- und Überwachungssystemen für bestandsgefährdende Entwicklungen der Gesellschaft.
- Der Begriff **Code of Conduct** beinhaltet als Teil eines Compliance-Systems, Handlungs- und Verhaltensanweisungen an die Mitarbeiter.

- Desweiteren gibt es über die gesetzlichen Pflichten hinaus noch soziale und ethische Pflichten der Geschäftsführung, die unter dem Begriff **Corporate Social Responsibility/ Business Ethics** zusammengefasst werden. Während das Gesetz das ethische Minimum darstellt, geht die von der Gesellschaft geprägte Moral häufig darüber hinaus. Maßnahmen im Bereich Corporate Social Responsibility/Business Ethics werden gerne als Werbemaßnahmen von Unternehmen eingesetzt.

1.1 Corporate Governance

Die von der Bundesministerin für Justiz im September 2001 eingesetzte „Regierungskommission Deutscher Corporate Governance Kodex“ verabschiedete am 26. Februar 2002 den Deutschen Corporate Governance Kodex, der die gesetzlichen Regeln und anerkannten Standards sorgfältiger Unternehmensführung zusammenfassen soll. Der Kodex besitzt über die Entsprechenserklärung gemäß § 161 AktG (eingefügt durch das Transparenz- und Publizitätsgesetz, in Kraft getreten am 26.07.2002) eine gesetzliche Flankierung. Vorstand und Aufsichtsrat von börsennotierten Gesellschaften erklären danach jährlich, dass den vom Bundesministerium der Justiz im amtlichen Teil des elektronischen Bundesanzeigers bekannt gemachten Empfehlungen der „Regierungskommission Deutscher Corporate Governance Kodex“ entsprochen wurde und wird oder welche Empfehlungen nicht angewendet wurden oder werden.

Mit dem Deutschen Corporate Governance Kodex sollen die in Deutschland geltenden Regeln für Unternehmensleitung und -überwachung für nationale wie internationale Investoren transparent gemacht werden, um so das Vertrauen in die Unternehmensführung deutscher Gesellschaften zu stärken. Der Kodex adressiert alle wesentlichen – vor allem internationalen – Kritikpunkte an der deutschen Unternehmensverfassung, nämlich

- mangelhafte Ausrichtung auf Aktionärsinteressen;
- die duale Unternehmensverfassung mit Vorstand und Aufsichtsrat;
- mangelnde Transparenz deutscher Unternehmensführung;
- mangelnde Unabhängigkeit deutscher Aufsichtsräte;
- eingeschränkte Unabhängigkeit der Abschlußprüfer.

Seitdem der Deutsche Corporate Governance Kodex erstmalig in Kraft getreten ist, wurde zudem eine Reihe von Änderungen beschlossen, letztmalig mit Datum vom 14. Juni 2007

Von Gesellschaften mit beschränkter Haftung wird in Zukunft zunehmend – sei es von Kapitalgebern oder den Gerichten – verlangt werden, dass sie sich ebenfalls an die Empfehlungen des Deutschen Corporate Governance Kodex halten. Es ist davon auszugehen, dass Gerichte hinsichtlich der Beurteilung sorgfältiger Unternehmensführung – wenigstens mittelbar – zunehmend Wertungen des Deutschen Corporate Governance Kodex heranziehen werden

1.2 Code of Conduct/Code of Ethics

Ein sogenannter Code of Conduct bzw. ein Code of Ethics sollte integraler Bestandteil eines Compliance-Systems sein. Darunter versteht man auf der einen Seite Handlungs- und Verhaltensanweisungen an die Mitarbeiter, um so den Umgang der Mitarbeiter untereinander und gegenüber Dritten zu regeln. Zwar gibt es für die Einführung derartiger Richtlinien keine rechtliche Verpflichtung, die Entwicklungen im Ausland, insbesondere in den USA, die entsprechende Richtlinien schon lange kennen und teilweise rechtlich einfordern, haben aber auch hier das Bewusstsein für die Notwendigkeit eines Verhaltenskodex geschärft. Hinzu tritt die Erkenntnis der Unternehmen, dass im „Kampf" um die Anwerbung hochqualifizierten Personals, die Bewerber gerade auch den Umgang des Unternehmens mit seinen Mitarbeitern zu einem maßgeblichen Entscheidungskriterium bei der Wahl Ihrer künftigen Arbeitsstätte erhoben haben.

Aus rechtlicher Sicht wird man sich davor hüten müssen, Ethikrichtlinien aus dem angloamerikanischen Rechtsraum eins-zu-eins auf inländische Unternehmen zu übertragen. Dem steht dass deutsche Arbeitsrecht in zweifacher Hinsicht – nämlich auf individualvertraglicher Ebene und auf kollektivrechtlicher Ebene – entgegen. Eine Vielzahl von Regelungen eines Code of Ethics werden den Bestimmungen des § 87 Abs. 1 Nr. 1 BetrVG unterfallen, wonach der Betriebsrat in Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb mitzubestimmen hat.[1] Auf individualvertraglicher Ebene stellt sich daneben die Frage, ob die einzuführenden Regelungen noch vom Direktionsrecht des Arbeitgebers gedeckt sind, oder aber es einer einvernehmlichen Vereinbarung bedarf.[2] Vorgelagert dürfte sich immer die Frage stellen, ob die Regelung im Hinblick auf einen Eingriff in die Privatautonomie überhaupt zulässig ist – wie dies bspw. bei dem Verbot privater Liebesbeziehungen von Arbeitskollegen („Wal Mart") der Fall ist.[3]

1.3 Corporate Social Responsibility/Business Ethics

Corporate Social Responsibility (CSR) – also soziale Verantwortung des Unternehmens – richtet über die Vorgaben die das Gesetz als ethisches Minimum an die Unternehmen richtet, das Augenmerk auf den Standort und die Verantwortung des Unternehmens im gesellschaftlichen Umfeld. Die Unternehmen werden sich zunehmend auch bewusst, dass sie gesellschaftliche Verantwortung zu übernehmen haben, wobei insbesondere ökologische und soziale Aspekte in den Mittelpunkt gerückt werden.

---

1 Vgl. nur LAG Düsseldorf v. 14.11.2005 – 10 TaBV 46/05, NZA-RR 2006, 81 ff.

2 Vgl. zu diesen Problemen ausführlich S. 197 ff. und *Schreiner*, Compliance Report, Februar 2007, 5 f.

3 LAG Düsseldorf v. 14.11.2005 – 10 TaBV 46/05, NZA-RR 2006, 81 ff.

In den letzten beiden Jahren haben die Unternehmen daher auf diesem Gebiet ihre Aktivitäten enorm verstärkt, indem Sie Mitarbeiter entsprechend geschult oder ganze CSR Abteilungen eingerichtet haben. Auf der anderen Seite wurde das Thema auch von Non-Profit Organisationen aufgegriffen und vorangetrieben, Medienhäuser haben Rankings initiiert.[4]

Dabei ist die Erkenntnis gereift, dass entsprechendes Engagement nicht nur Selbstzweck ist, sondern durchaus einen positiven Effekt auf die Geschäftsentwicklung haben kann. Teilweise wird dieses Engagement als direktes Marketing Tool eingesetzt. Man denke nur an die BP Fernsehwerbung zum Thema Umweltschutz, oder aber die Verknüpfung des Kaufs von Krombacher Bier mit der Rettung des Regenwaldes, die der BGH in seinen Entscheidungen vom 26. Oktober 2006 als grundsätzlich zulässig eingestuft hat.[5]

1.4 Risk Management Systeme

Anknüpfungspunkt für die Pflicht der Einrichtung eines Früherkennungs- und Überwachungssystems für bestandsgefährdende Entwicklungen der Gesellschaft ist § 91 Abs. 2 AktG.

Die auf das KonTraG von 1998 zurückgehende Norm[6] formuliert damit eine Bestandssicherungspflicht des Vorstandes und konkretisiert insoweit einen Teilaspekt der allgemeinen Leitungsaufgabe des Vorstands.[7] Ohne dass die Vorschrift die Verpflichtung zur Einführung eines allgemeinen „risk management“ begründet, wie es Teile der Betriebswirtschaftslehre und der Prüfungspraxis verstehen,[8] hat der Vorstand gleichwohl Maßnahmen zu treffen, die es ihm ermöglichen, die umschriebenen Entwicklungen[9] frühzeitig zu erkennen (vgl. dazu sogleich unter 2.8).

---

4 Vgl. zu dieser Entwicklung: *Unger*, Compliance Report, Februar 2007, 2, 4.

5 BGH v. 26.10.2006 – I ZR 33/04 [Regenwaldprojekt I], NJW 2007, 919 ff.; BGH v. 26.10.2006 – I ZR 97/04 [Regenwaldprojekt II], MDR 2007, 598.

6 Art. 1 Nr. 9 KonTraG v. 27. April 1998 (BGBl. I, 786).

7 Vgl. RegBegr. BT-Drucks. 13/9712 Seite 15 liSp.

8 Vgl. *Hüffer*, AktG, 7. Aufl. 2006, § 91 Rn. 1, 9.

9 Beispielhaft nennt die Regierungsbegründung die Aufnahme risikobehafteter Geschäfte, Verstöße gegen Vorschriften der Rechnungslegung oder gegen sonstige gesetzliche Vorschriften, vgl. RegBegr. BT-Drucks. 13/9712 Seite 15 liSp.

2. Aufbau einer Compliance-Organisation als Pflicht der Geschäftsleitung?

Während teilweise Möglichkeiten zur Verbesserung der Compliance-Organisation freiwillig sind, gibt es für viele Bereiche eine rechtliche Pflicht zum Aufbau einer Compliance Organisation.

2.1 Pflichten der Geschäftsleitung

Die rechtliche Pflicht zum Aufbau einer Compliance Organisation folgt bereits aus dem Umstand, dass die vertretungsbefugten Organe von AG und GmbH gegenüber der Gesellschaft eine Vielzahl von Pflichten zu beachten haben. Die Verletzung dieser Pflichten kann sowohl zur persönlichen Haftung der Geschäftsleitung gegenüber der Gesellschaft sowie gegenüber Dritten wie auch zu einer Reihe weiterer Rechtsfolgen führen. Diese weiteren Rechtsfolgen können insbesondere strafrechtlicher Natur sein, Sanktionen des Ordnungswidrigkeitenrechts beinhalten, aber auch zu aufsichtsrechtlichen, steuerrechtlichen und gesellschaftsrechtlichen Konsequenzen führen.

Es kommen z. B. Vorwürfe der Untreue bei leichtfertiger Kreditvergabe in Betracht.[10] Des Weiteren steigt die Zahl der Tatbestände, die mit Bußgeld bedroht sind, weiter an. Bei den Geschäftsleitern eines Kreditinstituts oder eines Versicherungsunternehmens besteht zudem die Möglichkeit der Abberufung durch die Bundesanstalt für Finanzdienstleistungsaufsicht (vgl. § 36 KWG).

Geschäftsleiter müssen bei der Verletzung von Pflichten grundsätzlich auch mit der fristlosen Kündigung des Anstellungsvertrages und den sich daran anschließenden finanziellen Einbußen rechnen.

Im Folgenden sollen nunmehr exemplarisch einige wichtige Pflichtenbereiche der Geschäftsleitungsorgane aufgezeigt werden.

10 *Schmitt*, BKR 2006, 125 ff.

2.2 Allgemeine Sorgfalts- und Treuepflicht

Zunächst hat die Geschäftsleitung – ebenso wie die Gesellschafter – gegenüber der Gesellschaft und den Gesellschaftern allgemeine Sorgfalts- und Treuepflichten einzuhalten.[11] Die einzelnen Sorgfalts- und Treuepflichten sind überwiegend nicht kodifiziert, sondern sie leiten sich aus der Organstellung der Geschäftsleitung innerhalb der Gesellschaft ab. Dabei hat die Geschäftsleitung die Sorgfalt eines ordentlichen Geschäftsmannes an den Tag zu legen, vgl. §§ 93 Abs. 1 S. 1 AktG, 43 Abs. 1 GmbHG. Dazu zählt unter anderem die Pflicht zur ordnungsgemäßen Unternehmensleitung unter Einhaltung der durch Gesetz, Satzung und Anstellungsvertrag festgelegten Grenzen.

In diesem Zusammenhang ist die Geschäftsleitung insbesondere an die durch Satzung und Anstellungsvertrag vorgegebene Kompetenzordnung der Gesellschaft gebunden. Die Geschäftsleitung hat sämtliche Geschäfte der Gesellschaft im Interesse und zum Wohle der Gesellschaft wahrzunehmen und alles zu unterlassen, was die Gesellschaft schädigen könnte. Die Geschäftsleitung hat stets den wirtschaftlichen Vorteil der Gesellschaft zu verfolgen und ist grundsätzlich nicht berechtigt in Wettbewerb zur Gesellschaft zu treten und der Gesellschaft Geschäftschancen zum eigenen Wohle zu entziehen.[12] Bei Verletzung dieser Pflicht steht der Gesellschaft nicht bloß ein Unterlassungsanspruch gegenüber der Geschäftsleitung zu, sondern ihr steht auch ein Schadensersatzanspruch zu.

Aufgrund der Beachtung des Wohles der Gesellschaft als höchstem Gut, ist es dem Geschäftsführer einer GmbH auch strafbewehrt untersagt Betriebs- oder Geschäftsgeheimnisse der Gesellschaft unbefugt weiterzugeben, vgl. § 85 GmbHG. Die Geheimhaltungspflicht gilt dabei auch für den Vorstand einer AG, vgl. § 93 Abs. 1 S. 3 AktG.[13]

Ausfluss der Business Judgement Rule ist die Pflicht zur angemessenen Vorbereitung einer Geschäftsführerentscheidung durch Einholung der entscheidungsrelevanten Informationen und der sich daran anschließenden Abwägung von Risiken bei Treffen einer bestimmten Entscheidung.[14] Diese Pflicht kommt selbstverständlich nur bei unternehmerischen – also nicht gebundenen – Entscheidungen der Geschäftsleitung in Betracht. Solche unternehmerischen Entscheidungen beinhalten notwendigerweise eine von der Geschäftsleitung vorzunehmende Prognose. Sollte z. B. die Geschäftsleitung die Entscheidung treffen, ein anderes Unternehmen zu erwerben ohne zuvor ausreichende Informationen über das zu erwerbende Unternehmen eingeholt zu haben und bei Unklarheiten eine „Due Diligence“ durchgeführt zu haben, so stellt dies eine schadensersatzpflichtbegründende Pflichtverletzung der Geschäfts-

---

11 Vgl. nur *Baumbach/Hueck*, GmbHG, 18. Aufl. 2006, § 35 Rn. 38; Hüffer, AktG, 7. Aufl. 2006, § 93 Rn. 5.

12 *Baumbach/Hueck*, GmbHG, 18. Aufl. 2006, § 35 Rn. 42.

13 Vgl. hierzu auch *Hüffer*, AktG, 7. Aufl. 2006, § 93 Rn. 6 ff.

14 Vgl. *Heidel*, Aktienrecht und Kapitalmarktrecht, 2. Aufl. 2007, § 93 Rn. 98.

leitung dar.[15] Ebenso ist die Geschäftsleitung verpflichtet vor der Kreditvergabe an einen Dritten zunächst eine Kreditwürdigkeitsprüfung vorzunehmen.[16]

2.3 Überwachungspflichten/Risikokontrollpflichten

Da die Geschäftsleitung nicht alle Maßnahmen im Unternehmen selbst vorzunehmen braucht, was rein faktisch bei Überschreitung einer bestimmten Unternehmensgröße auch gar nicht mehr möglich wäre, ist die Geschäftsleitung befugt, einzelne Aufgabengebiete an Dritte (zumeist nachgeordnete Mitarbeiter) zu delegieren. Dabei hat die Geschäftsleitung jedoch verschiedene Überwachungs- und Risikokontrollpflichten wahrzunehmen.

Bei der Delegation von Aufgaben hat die Geschäftsleitung insbesondere für die ordnungsgemäße Auswahl der Mitarbeiter, eine den übertragenen Aufgaben entsprechende Einweisung und eine ordnungsgemäße Überwachung der entsprechenden Mitarbeiter einzustehen.[17] Die Auswahl des Mitarbeiters hat erst nach vorhergehender Prüfung der persönlichen Eignung (Zuverlässigkeit, Belastbarkeit) und der fachlichen Befähigung (Ausbildung, Qualifikation, Erfahrung) des Mitarbeiters durch die Geschäftsleitung zu erfolgen. Nach Auswahl hat die Geschäftsleitung den Delegierten in seinen Verantwortungsbereich einzuweisen und ihm die zur Bewältigung der übertragenen Aufgaben notwendigen Kenntnisse und sachlichen Mittel zur Verfügung zu stellen. Nachdem der Dritte die ihm übertragene Tätigkeit unter Beachtung der vorgenannten Grundsätze aufgenommen hat, ist die Geschäftsleitung noch immer nicht aus ihrer Pflicht entlassen. Denn die Geschäftsleitung darf nicht blind auf die pflichtgemäße Erfüllung der übertragenen Aufgaben durch den Dritten vertrauen, sondern im Rahmen des objektiv Zumutbaren hat die Geschäftsleitung die Tätigkeit des Mitarbeiters ständig zu überwachen.[18]

Dies gilt grundsätzlich auch bei einer Aufteilung von verschiedenen Ressorts innerhalb der Geschäftsleitung. Der jeweilige Geschäftsführer oder das Vorstandsmitglied bleibt für die Überwachung ressortfremder Geschäftsführer und Vorstandsmitglieder verantwortlich, obwohl bei ordnungsgemäßer Geschäftsverteilung nur das zuständige Geschäftsleitungsorgan die volle Handlungsverantwortung trägt.[19] Sollten Zweifel an der Zuverlässigkeit des Mitgeschäftsführers entstehen, so sind die übrigen Geschäftsführer gegebenenfalls verpflichtet, den gesamten übertragenen Aufgabenbereich in das Gesamtgremium zurückzuholen. Des Weiteren sind die übrigen Geschäftsführer verpflichtet, etwaigen pflichtwidrigen Entscheidungen des Mitgeschäftsführers zu widersprechen.

---

15 Vgl. OLG Oldenburg v. 22.6.2006 – 1 U 34/03, GmbHR 2006, 1263 ff.

16 Vgl. zur strafrechtlichen Verantwortlichkeit BGH v. 15.11.2001 – 1 StR 185/01, NJW 2002, 1211 ff.

17 Sehr weitgehend BGH v. 21.1.1997 – VI ZR 338/95, NJW 1997, 1237 ff.

18 *Schmidt-Husson,* in: Hauschka (Hrsg.), Corporate Compliance, 2007, § 7 Rn. 24.

19 Vgl. *Hüffer*, AktG, 7. Aufl. 2006, § 93 Rn. 13a; *Lutter/Hommelhoff*, GmbHG, 16. Aufl. 2004, § 43 Rn. 17.

Zu den Überwachungs- und Risikokontrollpflichten der Geschäftsleitung zählt auch das nach § 91 Abs. 2 AktG durch den Vorstand einer AG zu installierende Frühwarnsystem, welches später noch näher behandelt und erläutert wird.

2.4 Buchführungs-/Bilanzierungspflichten

Nach § 238 HGB ist jeder Kaufmann verpflichtet, Bücher zu führen und in diesen sein Handelsgeschäfte und die Lage seines Vermögens nach den Grundsätzen ordnungsgemäßer Buchführung darzustellen. Als Formkaufmann sind die Kapitalgesellschaften Normadressat der Bestimmung des § 238 HGB. Aus § 264 HGB folgt die Verpflichtung der gesetzlichen Vertreter einer Kapitalgesellschaft, also Vorstand und Geschäftsführung, zur Rechnungslegung. Die Rechnungslegung umfasst nach den §§ 238 ff. HGB die Vornahme der Inventur, die Aufstellung der (Eröffnungs-)Bilanz, die Aufstellung der Gewinn- und Verlustrechnung sowie die Anfertigung des Anhangs und des Lageberichts. Zwar ist auch die Rechnungslegungspflicht rein faktisch auf Dritte (z. B. externe Berater) übertragbar, allerdings haftet der Vorstand bzw. die Geschäftsführung gem. §§ 91 Abs. 1 AktG, 41 Abs. 1 GmbHG für die ordnungsgemäße Erfüllung dieser Verpflichtung.[20]

Nach § 325 HGB haben die gesetzlichen Vertreter einer Kapitalgesellschaft auch den Jahresabschluss (größenabhängige Erleichterungen ergeben sich aus den §§ 326 ff. HGB i.V.m. § 267 HGB) beim Betreiber des elektronischen Handelsregisters einzureichen. Die haftungsrechtliche Verantwortlichkeit für die ordnungsgemäße Buchführung kann dabei weder durch die Satzung noch durch einen entsprechenden Beschluss der Haupt- oder Gesellschafterversammlung auf Dritte übertragen werden, so dass sich die Geschäftsführung letztendlich nicht der umfangreichen Verantwortung entziehen kann und aus diesem Grund zumindest die bereits oben beschriebenen Überwachungsaufgaben wahrzunehmen hat.

Bei Verletzung der Rechnungslegungspflichten drohen sowohl steuerrechtliche Konsequenzen (vgl. beispielhaft §§ 162, 370 Abs. 1 AO) als auch ordnungs- und strafrechtliche Sanktionen (vgl. §§ 331, 335 HGB, 283 Abs. 1 Nr. 5-7, 283 a, 283 b StGB).

2.5 Gesellschaftsrechtliche und öffentlich rechtliche Pflichten

Darüber hinaus treffen die gesetzlichen Vertreter von Kapitalgesellschaften auch gesellschaftsrechtliche Pflichten, wie etwa die Verpflichtung zur Anmeldung eintragungsrelevanter Tatsachen beim zuständigen Handelsregister (vgl. z. B. §§ 181, 188 AktG, 40 GmbHG). Un-

---

[20] Vgl. für die AG: *Hüffer*, AktG, 7. Aufl. 2006, § 91 Rn. 2.

terlässt der Verpflichtete die Vornahme von anmeldepflichtigen Tatsachen, so droht insbesondere die Zwangsgeldverhängung gegen die Mitglieder der Geschäftsführung, vgl. §§ 407 Abs. 1 AktG, 79 GmbHG.

Weiterhin sind die Vertretungsorgane der Kapitalgesellschaften zur Vorbereitung und Einberufung von Gesellschafterversammlung und Hauptversammlung verpflichtet (vgl. §§ 121 Abs. 2 AktG, 49 Abs. 1 GmbHG) sowie zur Durchsetzung der dort getroffenen Beschlüsse.

Darüber hinaus bestehen sehr weitgehende zusätzliche Verpflichtungen der Geschäftsführung. Dazu zählen insbesondere die Pflicht zur Abführung der Steuern (wozu die gesetzlichen Vertreter persönlich verpflichtet sind, vgl. §§ 34, 69 S. 1 AO), die Pflicht zur fristgerechten Abführung von Sozialversicherungsbeiträgen und schließlich die Pflicht bei Zahlungsunfähigkeit oder Überschuldung rechtzeitig Insolvenzantrag zu stellen (vgl. §§ 92 Abs. 2 AktG, 64 Abs. 1 GmbHG).

Bei Erreichen bestimmter Beteiligungsschwellen an einer börsennotierten Gesellschaft ist die Geschäftsführung gegenüber der Bundesanstalt für Finanzdienstleistungen nach dem Gesetz über den Wertpapierhandel (WpHG) zur Anzeige verpflichtet, vgl. § 21 Abs. 1 WpHG.

Zusätzlich ist der Vorstand einer AG zur regelmäßigen Berichterstattung an den Aufsichtsrat hinsichtlich der beabsichtigten Geschäftspolitik und der Wirtschaftlichkeit der laufenden Geschäfte verpflichtet, vgl. § 90 Abs. 1 AktG. Vorstand und Aufsichtsrat von börsennotierten Gesellschaften haben gem. § 161 AktG einmal jährlich eine Entsprechenserklärung abzugeben, ob und inwieweit den von der Regierungskommission Deutscher Corporate Governance Kodex gemachten Empfehlungen entsprochen wurde. Nach § 15 WpHG ist der Vorstand zur Veröffentlichung von Tatsachen verpflichtet, wenn sie wegen ihrer Auswirkungen auf die Vermögens- oder Finanzlage oder auf den allgemeinen Geschäftsablauf geeignet sind, den Börsenpreis der Aktie zu beeinflussen. Bei Geschäften mit Aktien der Gesellschaft ist der Vorstand gegenüber der Gesellschaft und der Bundesanstalt für Finanzdienstleistungen offenlegungspflichtig, vgl. § 15 a WpHG.

2.6 Verpflichtung auf Compliance

Aus der lediglich exemplarischen Aufzählung der oben beschriebenen Pflichten der Geschäftsleitung folgt bereits in ihrem Interesse die Notwendigkeit der Einrichtung einer Compliance Organisation. Aufgrund der zunehmenden Anzahl von Haftungstatbeständen kann sich die Geschäftsleitung letztendlich nur durch Schaffung einer funktionierenden Struktur zur Einhaltung der gesetzlichen Verpflichtungen gegenüber der Gesellschaft und/oder Dritten absichern. Insbesondere geht es aber bei der Schaffung einer funktionierenden Compliance Organisation darum, den langfristigen Unternehmenserfolg zu sichern. Unternehmen, die durch eine gut funktionierende Compliance Organisation rechtliche Fehlerquellen und Zwischenfälle durch Rechtsverstöße minimieren, werden hiervon generell profi-

tieren, (i) durch den verbesserten internen Informationsfluss und Kontrollmaßnahmen, (ii) durch frühzeitiges Entdecken (auch nicht rechtlicher) Fehler, (iii) durch eine bessere Außenwirkung gegenüber Kunden und Dritten.

2.7 Informationsorganisation

Mit seinem Urteil vom 15. Dezember 2005[21] hat der BGH die Notwendigkeit der Einrichtung einer unternehmensinternen Informationsorganisation betont. Das Unternehmen habe durch organisatorische Maßnahmen zu gewährleisten, dass eine Information alle Stellen des Unternehmens erreicht, für die diese Information relevant sein kann.

Dem Urteil lag ein Fall zugrunde, in dem trotz einer über das Vermögen eines Schuldners im Insolvenzverfahren veröffentlichten Verfügungsbeschränkung dieser Schuldner ein Bankkonto eröffnete und über die dort eingehenden Beträge verfügte. Der BGH ging davon aus, dass die Bank die Verfügungsbeschränkungen seit dem Wirksamwerden der Veröffentlichung im Amtsblatt gekannt hat. Aufgrund der Vermutungswirkung, die durch die Veröffentlichung entstand (vgl. §§ 82 Satz 2, 9 Abs. 3 InsO) war es an der Bank zu beweisen, dass ihr die Verfügungsbeschränkung unbekannt war.

Dieser Beweis ist ihr insbesondere deshalb nicht gelungen, weil Sie eine funktionierende Informationsorganisation nicht darlegen konnte. Der BGH forderte von der Bank den Nachweis einer organisatorischen Vorsorge, damit ihre Kunden betreffende Informationen über die Eröffnung von Insolvenzverfahren oder Sicherungsmaßnahmen im Vorfeld der Insolvenzeröffnung von ihren Entscheidungsträgern zur Kenntnis genommen werden.

Diese Verpflichtung ist in einer entsprechenden, wegen der Möglichkeiten des Zugriffs auf Datenspeicher auch zumutbaren Organisation dergestalt umzusetzen, dass ein Informationsfluss in alle Richtungen gewährleistet ist. Erforderlich ist also zunächst ein Informationsfluss von oben nach unten. Umgekehrt müssen Erkenntnisse, die von einzelnen Angestellten gewonnen werden, jedoch auch für andere Mitarbeiter und spätere Geschäftsvorgänge erheblich sind, die erforderliche Breitenwirkung erzielen. Dazu kann auch ein horizontaler und filialübergreifender Austausch erforderlich sein.[22]

Die Konsequenzen, die der BGH aus dem Fehlen einer entsprechenden Organisation zieht, sind erheblich: „Jedenfalls dann, wenn es an derartigen organisatorischen Maßnahmen fehlt, muss sich die Bank das Wissen einzelner Mitarbeiter – auf welcher Ebene auch immer diese angesiedelt sind – zurechnen lassen“. Diese Aussage des BGH kann – wenn man darin nicht lediglich die Aussage sehen möchte, dass sich die Bank all das Wissen zurechnen lassen

---

21 BGH v. 15.12.2005 – IX ZR 227/04, NJW-RR 2006, 771 ff.

22 Vgl. BGH v. 1.6.1989 – III ZR 261/87, WM 1989, 1364, 1367; BGH v. 15.1.2004 – IX ZR 152/00, WM 2004, 720, 722.

muss, das ihr bei sachgerechter Organisation zur Verfügung gestanden hätte – auch dahingehend verstanden werden, dass eine Wissenszurechnung davon abhängt, welche Vorkehrungen das Unternehmen getroffen hat, um einen angemessenen Informationsaustausch in vertikaler und horizontaler Richtung zu ermöglichen.

Die Wissenszurechnung würde damit von einem Verschuldenselement abhängig gemacht. Jedenfalls dann, wenn das Unternehmen zu wenig getan hat, um seiner Verpflichtung zur Gewährleistung einer angemessenen Informationsorganisation nachzukommen, wird der juristischen Person alles Wissen zugerechnet, was einem Mitarbeiter gleich auf welcher Ebene bekannt ist. Im Umkehrschluss kann man daraus schließen, dass sich die juristische Person vor Wissenszurechnungen dann schützen kann, wenn sie einen solchen Informationsfluss nachweisen kann. Dass diese Grundsätze nur auf Banken beschränkt aufgestellt wurden, ist dem Urteil nicht zu entnehmen. Plausible Gründe wird man für eine Differenzierung auch nicht angeben können.

Deshalb tun Unternehmen gut daran, eine Organisation vorzuhalten, die für einen geregelten Informationsfluss innerhalb des Unternehmens sorgt. Denn Sie beugen damit in zweifacher Hinsicht möglichen Schäden vor: Zum einen können Fehler vermieden werden, weil die Entscheidungsträger die richtigen Informationen zugrunde legen. Zum Zweiten führt eine nachgewiesen gute Informationsorganisation zu größeren Entlastungsmöglichkeiten, wenn es um Wissenszurechnung geht. Wenn also eine Information trotz einer guten Vorsorge gleichwohl nicht an die richtige Stelle gelangt, wird diese Information – wenn man den Gedanken des BGH konsequent zu Ende denkt – auch nicht mehr zugerechnet.

2.8 Notwendigkeit der Einrichtung einer Abteilung „Interne Revision“[23]

Wie bereits oben dargestellt ist Anknüpfungspunkt für die Pflicht der Einrichtung eines Früherkennungs- und Überwachungssystems für bestandsgefährdende Entwicklungen der Gesellschaft die Vorschrift des § 91 Abs. 2 AktG.

2.8.1 Früherkennungs- und Überwachungssystem (§ 91 Abs. 2 AktG)

Die Maßnahmen, die der Vorstand ergreift, müssen geeignet sein, die Früherkennung zu gewährleisten. „Dazu gehört namentlich, die frühzeitige und umfassende Kenntnis des Vorstands sicherzustellen, und zwar des Gesamtvorstands, nicht nur seines Vorsitzenden oder

[23] Vgl. hierzu umfassend: *Berwanger/Kullmann*, Interne Revision – Wesen, Aufgaben und rechtliche Verankerung, 2008.

bestimmter Ausschüsse oder Arbeitsgruppen".[24] Frühzeitig ist die Kenntniserlangung dann, wenn eine nachteilige Entwicklung noch so rechtzeitig dem Vorstand bekannt wird, dass dieser der Entwicklung entgegenwirken und so eine Bestandsgefährdung abwenden kann.[25]

Wie bei anderen Leitungsentscheidungen auch hat der Vorstand ein Leitungsermessen insbesondere hinsichtlich der Art und Form der zu ergreifenden Maßnahmen. Das Ermessen ist am Maßstab der konkreten Umstände im Unternehmen (Größe, Branche, Risikopotenzial der Märkte, Struktur, Lage des Unternehmens, Kapitalmarktzugang) und der dort in Betracht kommenden nachteiligen Entwicklungen auszuüben.[26]

Was den neben den „Maßnahmen" angesprochenen zweiten Aspekt der Norm – dem Überwachungssystem – betrifft, herrscht Unklarheit, ob das System zur Überwachung der eingeleiteten Maßnahmen (so die überwiegende Ansicht) dient oder aber die risikoträchtigen Entwicklungen selbst zu überwachen sind. Da letztlich dem Begriff der „geeigneten Maßnahmen" auch die Einrichtung einer informationsvermittelnden Organisation zuzuordnen sein wird, dürfte die dargelegte Unklarheit für die Praxis kaum eine Rolle spielen.[27]

Das Überwachungssystem meint daher eine unternehmensinterne Kontrolle, die sicherstellen soll, dass die zur Früherkennung eingeleiteten Maßnahmen auch greifen, dass also die im Rahmen der Früherkennung gewonnenen Erkenntnisse zeitnah an den Vorstand weitergeleitet werden. Im Ergebnis wird man § 91 Abs. 2 AktG daher als eine Organisationsanforderung zu verstehen haben. Durch klar abgegrenzte Zuständigkeiten, ein engmaschiges Berichtswesen und eine entsprechende Dokumentation der Vorgänge wird man daher den Anforderungen genügen.

In der Regel dürfte zu einem angemessenen Überwachungssystem die Interne Revision sowie eine Controlling-Abteilung gehören.[28] Auch hier kommt es für die Frage der Ausgestaltung aber entscheidend auf die Größe,[29] Struktur und Lage des Unternehmens, das Risikopotential der Märkte, auf dem das Unternehmen tätig ist, sowie die Art des Kapitalmarktzugangs an. Keineswegs kann aus § 91 Abs. 2 AktG etwa eine konkrete Zuständigkeit oder Ablauforganisation der Risikoerfassung gefolgert werden, etwa bis hin zum Erfordernis von Schadensformularen etc. – dies mag betriebswirtschaftlich sinnvoll sein, rechtlich zwingend ist es nicht. Die Praxis sollte sich gleichwohl darauf einstellen, dass Einrichtungen geschaffen werden müssen, die die Funktion der bestehenden Controlling- und Revisionseinrichtungen des Unternehmens überwachen und eine kurzfristige Information des Vorstands sicherstellen.[30]

---

24 *Hüffer*, NZG 2007, 47, 49.

25 RegBegr. BT-Drucks. 13/9712 Seite 15 reSp.

26 *Hefermehl/Spindler*, in: MüKo/AktG 2. Aufl. 2004, § 91 Rn. 20.

27 *Hefermehl/Spindler*, in: MüKo/AktG 2. Aufl. 2004, § 91 Rn. 22.

28 *Hefermehl/Spindler*, in: MüKo/AktG 2. Aufl. 2004, § 91 Rn. 24.

29 Als Indiz wird man hier die in § 267 HGB aufgeführten Größenklassen mit heranziehen können.

30 *Hüffer*, NZG 2007, 47, 49.

Für Kreditinstitute und Finanzdienstleistungsinstitute besteht mit § 25 a KWG eine aufsichtsrechtliche Sonderregelung, die von den Instituten eine ordnungsgemäße Geschäftsorganisation verlangt, die die Einhaltung der von den Instituten zu beachtenden gesetzlichen Bestimmungen gewährleistet. Nach § 25 a Abs. 1 Nr. 1 KWG umfasst eine ordnungsgemäße Geschäftsorganisation insbesondere ein angemessenes Risikomanagement. Dies beinhaltet auf der Grundlage von Verfahren zur Ermittlung und Sicherstellung der Risikotragfähigkeit die Festlegung von Strategien sowie die Einrichtung interner Kontrollverfahren, die aus einem internen Kontrollsystem und einer internen Revision bestehen, wobei das interne Kontrollsystem dabei insbesondere umfasst:

- Aufbau- und ablauforganisatorische Regelungen, die eine klare Abgrenzung der Verantwortungsbereiche umfassen, und
- Prozesse zur Identifizierung, Beurteilung, Steuerung sowie Überwachung und Kommunikation der Risiken; dabei soll den in Anhang V der Bankenrichtlinie niedergelegten Kriterien Rechnung getragen werden."

Entsprechend dürfte man in diesen Wirtschaftsbereichen über die sich aus § 91 Abs. 2 AktG ergebenden Anforderungen hinaus ohne ein „risk management", ohne Compliance-Regelungen und ohne ablaufimmanente Kontrollen nicht auskommen.[31]

Interessant ist diese Vorschrift insbesondere im Hinblick auf ihr Verhältnis zu § 91 Abs. 2 AktG. Die ganz überwiegende Ansicht möchte diese Vorschrift zwar nicht branchenübergreifend zur Konkretisierung des § 91 Abs. 2 AktG heranziehen, hält aber eine entsprechende Berücksichtigung für zulässig.[32] Andererseits hat die Rechtsprechung die Norm schon zur Ausfüllung des § 91 AktG auch bei branchenfremden Unternehmen herangezogen.[33] In seiner Entscheidung vom 8. Juli 2004 war das Verwaltungsgericht Frankfurt a. M. der Ansicht „dass sich diese Norm [d.h. § 91 Abs. 2 AktG, Anm. d. Verf.] und § 25a Abs. 1 KWG [in] ihrer rechtlichen Bedeutung entsprechen […], so dass die in § 25a KWG gesetzlich genauer gefassten Anforderungen bei der Auslegung des § 91 Abs. 2 AktG herangezogen werden können […]. Diese weitgehende Sichtweise entspricht nach Auffassung der erkennenden Kammer der Gesamtintention des Gesetzgebers der […] die Verpflichtung der Geschäftsleitung hervorheben wollte, Risikofrüherkennungs- sowie Risikoüberwachungssysteme in den Unternehmen einzurichten, um Entwicklungen vorzubeugen, die den Fortbestand der Gesellschaft gefährden können".[34] Auch wenn die nachfolgende Argumentation des Gerichts darauf hindeuten könnte, dass man die entsprechende Heranziehung des § 25a KWG nur auf Versicherungsunternehmen erstrecken möchte, wird sich die Praxis sicherheitshalber auch an den Vorgaben des § 25a KWG orientieren müssen.

---

31 *Hüffer*, ebd.

32 *Hüffer*, ebd. m.w.N.

33 VG Frankfurt a.M. v. 8. Juli 2004 – 1 E 7363/03 (I), WM 2004, 2157, 2160.

34 Ebd.

2.8.2 Ausstrahlungswirkung auf GmbH?

Inwieweit § 91 Abs. 2 AktG, der grundsätzlich nur auf Vorstände von Aktiengesellschaften Anwendung findet, auch auf andere Gesellschaftsformen zu übertragen ist, wird – jedenfalls was das Ausmaß der Auswirkungen betrifft – unterschiedlich beurteilt. Der Gesetzgeber hat eine Ausstrahlungswirkung – ohne deren konkrete Reichweite darzulegen – ausdrücklich formuliert:

> *„In das GmbHG soll keine entsprechende Regelung aufgenommen werden. Es ist davon auszugehen, dass für Gesellschaften mit beschränkter Haftung je nach ihrer Größe, Komplexität ihrer Struktur usw. nichts anderes gilt und die Neuregelung Ausstrahlungswirkung auf den Pflichtenrahmen der Geschäftsführer auch anderer Gesellschaftsformen hat".*[35]

Da der Gesetzgeber jedoch – obwohl es ihm leicht gefallen wäre – keine entsprechende Regelung in das GmbHG eingeführt hat, wird man auch eine gänzlich gleichlaufende Verpflichtung nicht annehmen dürfen. Auch die Struktur bspw. der GmbH mit einem dem Vorstand gegenüber nicht ähnlich starken, nämlich weisungsgebundenen Leitungsorgans widerspricht einer „eins-zu-eins" Übertragung. Vielmehr wollte der Gesetzgeber die Reichweite der Norm der weiteren Entwicklung in Rechtsprechung und Literatur überlassen.[36] Andererseits lässt sich schon aus § 43 Abs. 1 GmbHG ableiten, dass den Geschäftsführer die Verpflichtung trifft, sich um die rechtzeitige Erkennung von Krisen-Anzeichen zu bemühen.[37] Schon ohne einen Rückgriff auf die Norm des § 91 Abs. 2 AktG wird sich ein Geschäftsleiter nur dann – bei Nichteinrichtung einer Abteilung „Interne Revision" – der Haftung entziehen können, wenn er auf ausreichender Informationsbasis eine den Gegebenheiten des Unternehmens angemessene Ermessensentscheidung über Einführung, Augestaltung und Umfang einer internen Kontrolle trifft.[38]

Bei dieser Entscheidung ist jedoch die gesetzgeberische Intention in § 92 Abs. 2 AktG mit zu berücksichtigen. Wenn auch die Reichweite der Ausstrahlung unklar ist, ist man sich doch einig, dass die Norm auch in andere Rechtsformen hineinwirkt. Der Gesetzgeber hat aber deutlich gemacht, dass er grundsätzlich auf eine Einrichtung derartiger Maßnahmen und entsprechender Überwachungssysteme hinarbeitet. Dies bedeutet für die Geschäftsleiter, dass sie sich von vornherein einem erhöhten Rechtsfertigungsdruck aussetzen, wenn sie sich gegen die Einrichtung entsprechender Systeme entscheiden.

Die Notwendigkeit der Einrichtung einer Abteilung „Interne Revision" wird man für die GmbH daher erst dann aus § 91 Abs. 2 AktG ableiten können, wenn diese dem in § 91 Abs. 2 AktG zugrundegelegten Leitbild eines komplexen Großunternehmens so stark entspricht,

---

35 RegBegr. BT-Drucks. 13/9712 Seite 15 reSp.

36 *Drygala/Drygala*, ZIP 2000, 297, 300 mwN.

37 *Westermann*, DZWIR 2006, 485, 387.

38 In diese Richtung argumentierend *Drygala/Drygala*, ZIP 2000, 297, 303 f. Nur klarstellend ist festzuhalten, dass es in der Frage, ob nachgeordnete Entscheidungsebenen von der Führungsebene zu überwachen sind, sicherlich kein unternehmerisches Leitungsermessen gibt, allerdings ist es eine andere Frage, ob eine derartige Überwachung in der von § 91 Abs. 2 AktG angestrebten Organisationsstruktur umzusetzen ist.

dass eine Nichtanwendung der aktienrechtlichen Vorschrift systemwidrig wäre.[39] Wie bei der Aktiengesellschaft kommt es damit auch bei der GmbH letztlich auf eine Unternehmensangemessene Organisationsstruktur an, die je nach Größe, Struktur und Risikopotential des Unternehmens auszugestalten ist.

Praxishinweis

Kann das Unternehmen – auch wenn es in der Rechtsform der GmbH besteht – nach den in der Regierungsbegründung beispielhaft genannten Faktoren (Struktur, Größe o. ä.) dem Kreis der Unternehmen zugeordnet werden, die einer Aktiengesellschaft entsprechen, wie sie § 91 Abs. 2 AktG vor Augen hat, spricht vieles dafür, auch in einer Gesellschaft in der Rechtsform einer GmbH eine interne Revision einzurichten. Vorzugsweise dürften mit Hilfe eines externen Beraters zunächst die revisionsrelevanten Risken zu identifizieren sein, um eine entsprechende Themenliste für die Interne Revision und entsprechend die notwendigen Kapazitäten der Revisionsabteilung herausarbeiten zu können.

Kommt die Geschäftsleitung ihren dergestalt ausgeformten Verpflichtungen aus § 91 Abs. 2 AktG nicht nach, haften die Vorstandsmitglieder der Gesellschaft gegenüber gemäß § 93 Abs. 2 S. 1 AktG. Die Nichteinhaltung der Pflichten nach § 91 Abs. 2 AktG kann zudem ein wichtiger Grund zur Abberufung und fristlosen Kündigung sein. Für die Geschäftsleitung einer GmbH könnte man – wenn man § 91 Abs. 2 AktG in seiner Ausstrahlungswirkung als Konkretisierung des § 43 Abs. 1 GmbHG verstehen möchte – eine Haftung nach § 43 Abs. 2 GmbHG annehmen.

3. Umsetzung einer Compliance Organisation

Außer der Einrichtung einer internen Revision als Teil einer Compliance Struktur – zumindest für große Unternehmen – gibt es weitere organisatorische Möglichkeiten, die Compliance Struktur im Unternehmen zu verbessern.

---

[39] *Veil*, ZGR 2006, 374, 376 f. m.w.N.; *Drygala/Drygala*, ZIP 2000, 297, 305; noch strenger *Altmeppen*, ZGR 1999, 291, 301 f.

3.1 Planung der Compliance Organisation

Für die Planung der Compliance-Organisation sollte zunächst im Rahmen einer unternehmensinternen „Due Diligence" eine Art Bestandsaufnahme bereits bestehender Abläufe und Überwachungssysteme durchgeführt werden. Im Anschluss sollten die Ziele des Gesamtprojekts definiert und die grundsätzliche Herangehensweise festgelegt werden.

3.1.1 Baukastensystem vs. Komplettlösung

Je nachdem welches Überwachungssystem im Unternehmen bereits etabliert ist und welche Faktoren für das Unternehmen eine Rolle spielen (Größe/Branche/Risikopotential der Märkte), muss entschieden werden, ob die Einführung einer umfassenden „Komplettlösung/ Teilsysteme" erforderlich ist. Vorhandene Systeme müssen auf Einheitlichkeit von Abläufen und eventuelle Verknüpfbarkeit überprüft werden.

3.1.2 Identifikation Pflichtenkreise

Im Rahmen einer Due-Diligence oder Compliance Audit müssen die für das Unternehmen und seine Mitarbeiter relevanten Pflichtenkreise definiert werden. Hierbei gibt es **branchenunabhängige Pflichtenkreise** wie beispielsweise

- Arbeitssicherheit
- Allgemeine Gleichbehandlung
- Geräte- und Produktsicherheit
- Wettbewerbsrecht
- Datenschutzrecht
- Strafrecht (Integrität)
- Außenhandelsrecht
- Geldwäscherecht

Aus diesen Pflichtenkreisen resultierende Vorgaben und notwendigen Abläufe müssen definiert und Verantwortungsbereichen und somit auch Mitarbeiterkreisen zugeordnet werden. Ergänzend muss diese Vorgehensweise **für branchenbezogene Pflichtenkreise durchgeführt werden**. Beispiele hierfür sind:

- Umweltrecht (insb. Immissionsschutzrecht / Kreislaufwirtschafts- und Abfallrecht)
- Gentechnikrecht
- Arzneimittelrecht
- Kreditwesenrecht
- Versicherungsaufsichtrecht

Die aus diesen Pflichtenkreisen resultierenden Handlungsanweisungen, Verhaltensvorschriften Standards und Sanktionen können z. B. im Rahmen eines Handbuchs festgehalten und über Schulungsmaßnahmen den Mitarbeitern aufgezeigt werden (s. u.).

3.1.3 Entwicklung der Compliance-Struktur

Für das Grundgerüst einer Compliance Organisation werden stets einige Grundlagen zu beachten sein. Zunächst wird der Chief Compliance Officer („CCO“) dem Vorstandsvorsitzenden direkt unterstellt und berichtspflichtig sein müssen, um für eine weitgehende Unabhängigkeit im Unternehmen zu sorgen. Sofern erwünscht kann dem CCO ein unabhängiges Kontrollgremium (Compliance Committee) zur Seite gestellt werden, das aus externen Experten bestehen kann. Sofern als Teil der Compliance Organisation auch ein Ombudsmann im Rahmen einer Whistle-Blowing Hotline installiert werden soll, wird dieser ähnlich dem CCO nur dem Vorstandsvorsitzenden berichtspflichtig sein müssen, um Unabhängigkeit zu gewährleisten. Selbstverständlich muss ein Austausch mit dem CCO hinsichtlich Compliance Verstößen gewährleistet sein. In den Stabsabteilungen und in allen weiteren Unterabteilungen sind jeweils für die Überwachung der Compliance verantwortliche Mitarbeiter zu benennen, welche natürlich auch entsprechend zu schulen sind. Auf allen Ebenen besteht die Pflicht zur eigenständigen Überwachung und Kontrolle im eigenen Verantwortungsbereich. Entsprechend sollte eine Dokumentationspflicht über die Compliancetätigkeit bestehen. Die Struktur einer Compliance Organisation könnte beispielsweise folgendermaßen aussehen:

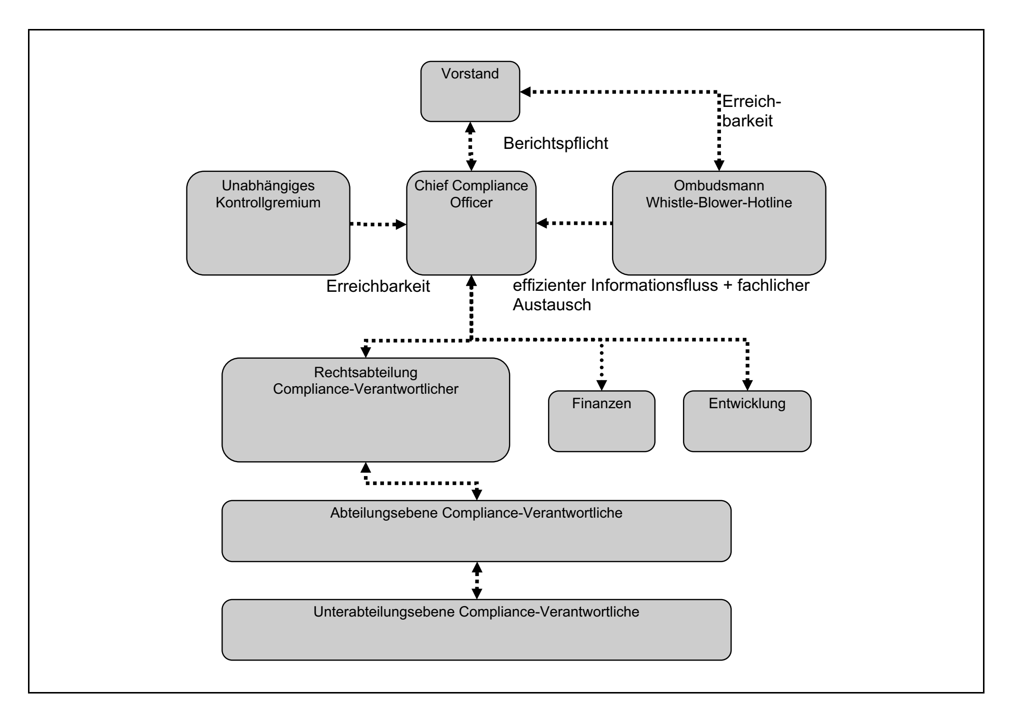


Abbildung 1: *Struktur einer Compliance Organisation*[40]

3.2 Handbücher und Compliance Systeme

Zur Begrifflichkeit und Grundlage eines sog. Code of Conduct bzw. Code of Ethic wurde bereits oben Stellung genommen.

3.2.1 Compliance Handbücher

Handbücher können ein sinnvoller Baustein einer Compliance Struktur sein. Wichtig ist hierbei zunächst eine genaue Festlegung der Adressatenkreise des Handbuchs. Sinnvoll sind neben allgemeinen Handlungs- und Verhaltensanweisungen, getrennte Handbücher für unterschiedliche Pflichtenkreise im Unternehmen, da sich etwa für die Produktion oder den Vertrieb völlig andere Pflichtenkreise ergeben können, als beispielsweise für die Verwaltung. Die genaue Zuordnung der gesetzlichen Pflichtenkreise und der Adressaten im Unternehmen ist daher Erfolgsvoraussetzung.

40 In Anlehnung an: *Rodewald/Unger*, BB 2007, 1629, 1632.

Da über Handbücher den Mitarbeitern die von ihnen zu beachtenden Pflichten und gesetzlichen Vorgaben erläutert werden, reicht es nicht aus, Handbücher bloß zur Verfügung zu stellen. Vielmehr muss sichergestellt und überprüft werden, dass jeder Mitarbeiter die für ihn geltenden Lektionen kennt. Es bietet sich daher an, die Mitarbeiter in Pflichtschulungen über die relevanten Pflichtenkreise zu schulen. Dies kann in herkömmlicher Art oder über Internet oder Telefonschulungen bewältigt werden. Bei der Auswahl des Schulungsmediums ist zu berücksichtigen, wie eine möglichst hundertprozentige Abdeckung der betroffenen Mitarbeiter sichergestellt werden kann. Je nach Unternehmen kann eine hohe Einbeziehungsquote am besten über Internetschulungen erreicht werden. Zudem haben solche „modernen" Schulungsmaßnahmen den Vorteil, dass jeder Mitarbeiter die Schulung zu einem ihm passenden Zeitpunkt am PC durchführen kann und ein minimaler Zeitaufwand hierfür notwendig ist. Die Vermeidung von Arbeitsausfall und Reisekosten ist bei der Entscheidung zwischen herkömmlicher Schulungsveranstaltung und eLearning sicher ein wichtiger Faktor, der ggf. mögliche Mehrkosten z. B. für eLearning-Programme ausgleichen kann.

3.2.2 IT- Systeme zur Sicherstellung der Compliance

Vision der Systemhersteller ist es, Compliance-Management Lösungen bereitzustellen, die dauerhaft die laufenden Compliance-Kosten senken. Hauptziele sind hierbei die Erfassung aller gesetzlichen Pflichten, die Rationalisierung und Sammlung von Compliance-Daten und die Erweiterung der Nachweisführung durchgeführter Compliance-Maßnahmen. Die Benutzerfreundlichkeit und die Verknüpfung mit weiteren Anwendungen wie z. B. einem integrierten Dokumentenmanagement spielen hierbei eine wichtige Rolle.

Beteiligungsmanagementsysteme

Beteiligungsmanagementsysteme können gerade bei großen Konzernen mit einer großen weltweiten Streuung von Tochterunternehmen für Transparenz trotz unglaublicher Daten- und Informationsdichte sorgen. Sind die Informationen erst eingepflegt, stehen sie weltweit auf Knopfdruck über die Internetoberfläche allen berechtigten Nutzern zur Verfügung.

Voraussetzung für ein erfolgreiches Beteiligungsmanagement ist jedoch, dass bei der Eingabe der entsprechenden Unternehmensdaten mit äußerster Sorgfalt vorgegangen wird. Werden Daten von zuvor genutzten alten Systemen einfach ungeprüft auf ein neues globales IT-System überspielt, werden auch die Fehler mit übernommen. Die Akzeptanz einer fehlerbehafteten Datenbank dürfte sich jedoch in Grenzen halten.

Für gesellschaftsrechtliche Kerninformationen empfiehlt sich daher bei der Einrichtung eines solchen Systems vor der Datenmigration zunächst eine Überprüfung (Due-Diligence) der Daten vorzunehmen.

Es bietet sich zudem an, Beteiligungsmanagementsysteme um weitere Komponenten einer Compliance Struktur zu ergänzen. Moderne Systeme bieten die Möglichkeit der Durchführung von Schulungen über das Internet an. Die heute am Markt verfügbaren Systeme bieten die technischen Möglichkeiten, um beispielsweise Schulungen für bestimmte Personenkreise durchzuführen und dies auch zu dokumentieren. Darüber hinaus bringt der Einsatz solcher Systeme eine enorme Datensicherheit und sorgt folglich in hohem Maße zur Verbesserung der Compliance im Unternehmen.

IT-Systeme und eLearning

Andere Systeme, wie beispielsweise ein kanadisches System, dienen vornehmlich der Überprüfung des aktuellen Compliance Maßstabs und ersetzen insofern in erster Linie händische Checklisten. Ähnlich wie bei den Compliance Handbüchern werden zunächst die Pflichtenkreise nebst konkret anwendbaren Vorschriften analysiert. Diese Analyse wird in den jeweiligen Ländern von Juristen durchgeführt. Anschließend werden die anwendbaren gesetzlichen Vorschriften in separat zuweisbare Aufgaben einzelner Führungskräfte übersetzt. Diese Führungskräfte werden dann über das Internet halbjährlich einer Prüfung unterzogen und müssen zu wichtigen Sachverhalten und Pflichten konkret Stellung nehmen. Dabei werden die gesetzlichen Vorschriften jeweils in vereinfachter Sprache dargestellt und es wird erklärt, warum welche gesetzliche Vorschrift einzuhalten ist. Die so abgelieferten Compliance-Berichte werden auf Übereinstimmung mit den gesetzlichen Vorschriften geprüft und gespeichert. Sofern Beanstandungen erforderlich sind, erhält die jeweilige Führungskraft eine Aufforderung zur Nachbesserung. Dieses System, das Schulung und Reporting verknüpft, wird zurzeit noch überwiegend von Versicherungsunternehmen und Banken in den USA und in Kanada genutzt.

4. Beispiele und Kontrollsysteme

Täglich vorkommende Pressemeldungen zu compliancebezogenen Vorkommnissen machen deutlich, dass das Thema Compliance bei vielen Unternehmen noch nicht mit letzter Konsequenz bearbeitet wird. Als Beispiel können die Korruptionsfälle bei Siemens und DaimlerChrysler, sowie die Vorfälle mit Sonderzahlungen und Vergnügungsreisen für Betriebsräte herangezogen werden. Laut Zeitungsmeldungen waren beispielsweise bei Siemens jeweils hoch in der Hierarchie angesiedelte Führungskräfte in diese Fälle verwickelt, allerdings liegen keine Indizien für eine Bereicherung der Manager zu Lasten ihres Arbeitgebers vor. Hieraus lässt sich wiederum schließen, dass die Manager glaubten, bei der Bestechung zur Erlangung von Aufträgen im Interesse ihres Unternehmens zu handeln. Gerade die zweite und dritte

Führungsebene kann man durch Schulungen leicht auf Verhaltensvorschriften einschwören. Hätte der Vorstand somit unmissverständlich über Verhaltensanweisungen zum Ausdruck gebracht, dass die Zahlung von Bestechungsgeldern dem Unternehmen schadet und zwingend zu unterlassen ist, wäre ein solcher Irrglauben der Manager eigentlich ausgeschlossen.

Hätte die Bank in dem vom BGH[41] entschiedenen und oben zum Thema Informationsorganisation dargestellten Fall ein System eingeführt, in welches Verfügungsbeschränkungen eingetragen und mit den Namen und Kontendaten von Kunden verknüpft werden, wäre es zu einem solchen Fall nicht gekommen.

Die Beispielsfälle zeigen, dass die notwendigen Compliance Maßnahmen für Unternehmen je nach Branche sehr unterschiedlich ausfallen können. Nicht immer sind IT-gestützte Lösungen der Weisheit letzter Schluss. Grundsätzlich gilt jedoch, dass moderne Systeme insbesondere für große Unternehmen eine ernorme Erleichterung darstellen können. Angefangen mit der Verbesserung der Datengenauigkeit durch Nutzung von Beteiligungsmanagement – oder Vertragsmanagementsystemen, über eLearning und Handbücher dürfte im Schadensfall eins jedenfalls immer gelten: Wer umfangreiche Maßnahmen getroffen hat, steht sowohl vor der Staatsanwaltschaft als auch in der Öffentlichkeit und bei Investoren besser dar. Zudem dürfte den Organen der Unternehmen die Möglichkeit vieler IT-Systeme, Compliance Maßnahmen genau zu dokumentieren, im Hinblick auf eine drohende Haftung bei unterlassener Überwachung sehr gelegen kommen.

5. Fazit

Als Fazit bleibt die Aussage: Arbeite ordentlich und dokumentiere, dass du ordentlich gearbeitet hast!

41 BGH v. 15.12.2005 – IX ZR 227/04, NJW-RR 2006, 771 ff.

Praxistipps Produkthaftung

Volker Steimle / Guido Dornieden

Zusammenfassung

Schlechtes Krisenmanagement beim Umgang mit einer Produktkrise kann für das betroffene Unternehmen in jeglicher Hinsicht teuer werden. Im „worst case“ endet sie in der strafrechtlichen Verantwortlichkeit der handelnden Personen. Ein gut aufgestelltes Unternehmen sorgt auch für diesen Ernstfall rechtzeitig vor – und entledigt sich durch ein vorausschauendes Handeln bereits im Vorfeld einer Vielzahl von Problemen. Der vorliegende Beitrag erläutert, woran hier im Einzelnen zu denken ist.

1. Einleitung

Produkthaftung stellt insbesondere in produzierenden Unternehmen ein sehr weites Feld dar. Die proaktive Vermeidung von Schäden und Risiken aus Produkthaftung – das Betätigungsfeld von „Compliance“ – verlangt nicht zuletzt deshalb sehr umfangreiche und komplexe Prozesse. Im Rahmen einer proaktiven Betrachtung sollte der Umgang mit Produkthaftung nicht auf die Produkthaftung im engeren rechtlichen Sinne begrenzt werden, sondern sämtliche Gefahren und Schäden aus schadhaften, riskanten, nicht regelkonformen oder sonstig schadensstiftenden Produkten mit umfassen. Ausgehend von der rechtlichen Natur möglicher Ansprüche gegen den Hersteller solcher Produkte, sind hier drei Rechtsquellen zu berücksichtigen: vertragliche Gewährleistung (etwa §§ 433 ff. BGB bei Kaufverträgen), Deliktsrecht (§§ 823 ff BGB) sowie das Produkthaftungsgesetz.

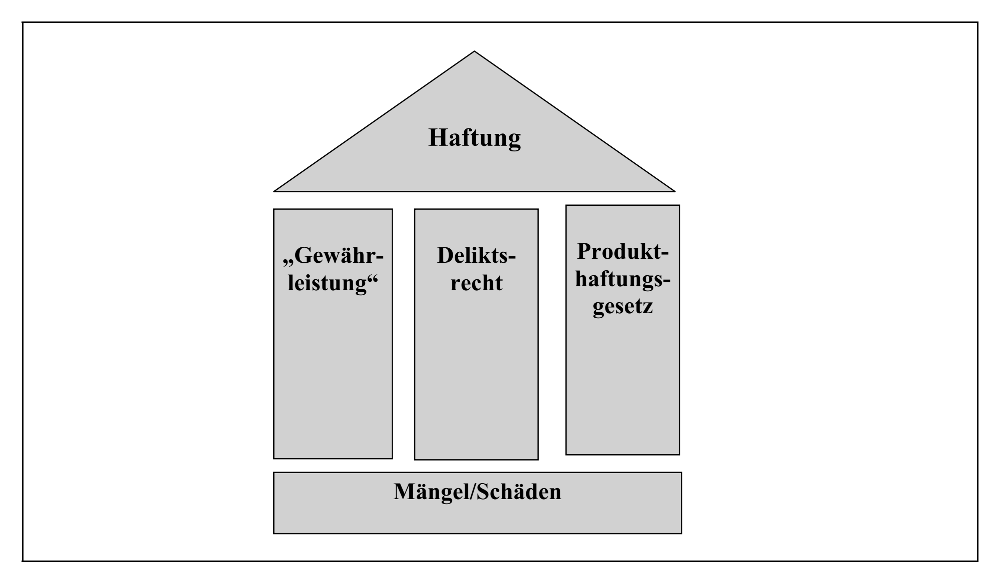


Abbildung 1: *Die drei Säulen der Produkthaftung*[1]

Diese drei möglichen Anspruchsgrundlagen zu Gunsten eines Geschädigten stehen im Wege der so genannten **Anspruchskonkurrenz** nebeneinander. Der Geschädigte hat folglich die freie Wahl, auf welche der verschiedenen Anspruchsgrundlage er die von ihm begehrte Rechtsfolge, etwa einen Anspruch auf Schadensersatz, stützen möchte. Das Wesen der Anspruchskonkurrenz hat darin seine innere Logik, dass die verschiedenen Anspruchsgrundlagen unterschiedliche Voraussetzungen, aber auch unterschiedliche Rechtsfolgen haben.[2] Je nach Lage des Einzelfalls kann es daher für einen Geschädigten erfolgversprechender sein, sich auf eine dieser Anspruchsgrundlagen zu stützen, die für ihn in der Rechtsverfolgung sicherer erscheint als eine andere der Anspruchsgrundlagen.

Vereinfacht ausgedrückt, sind die jeweiligen Ziele dieser Anspruchsgrundlagen folgende:

- **Vertragliche Gewährleistung:** Sicherstellung des vertraglich vereinbarten Gleichgewichts zwischen Leistung und Gegenleistung.
- **Deliktsrecht:** Schutz bestimmter, sogenannter „absoluter“ Rechtsgüter gegenüber jedermann (Leben, Gesundheit, Eigentum etc.)
- **Produkthaftungsgesetz:** Schutz von Leben, Gesundheit und in eingeschränktem Umfang Eigentum von Verbrauchern.

1 Abbildung aus *Steimle*, Vertragsrecht für Nichtjuristen (Convent-Seminare)

2 Bis zum Inkrafttreten des 2. Schadensersatzänderungsgesetzes vom 18. April 2002 war etwa Schmerzensgeld nur bei einer Haftung des Schädigers aus Deliktsrecht zu erhalten, nicht aber etwa aus verschuldensunabhängiger Gefährdungshaftung wie dem Produkthaftungsgesetz.

Während Ansprüche aus vertraglicher Gewährleistung zwar die Lieferung unsicherer Produkte zur Grundlage haben können, aber nicht müssen (die Lieferung eines pinkfarbenen Ferrari statt des georderten roten Sportwagens würde sicherlich Gewährleistungsansprüche begründen, ohne deswegen ein weniger sicheres Produkt darzustellen), greifen Deliktsrecht und Produkthaftungsgesetz immer nur dann ein, wenn unsichere Produkte Schäden verursachen bzw. zu verursachen drohen.

Neben diesen Rechtsquellen des Zivilrechts werden produkthaftungsrechtliche Fragen zunehmend auch durch das **öffentliche Recht** geprägt. Insbesondere das europarechtlich geprägte **Geräte- und Produktsicherheitsgesetz (GPSG)**[3] weist den jeweils zuständigen Aufsichtsbehörden weitreichende Befugnisse zu (inklusive der Befugnis, den Rückruf gefährlicher Produkte hoheitlich anzuordnen, Verbraucher öffentlich vor gefährlichen Produkten zu warnen oder das Inverkehrbringen bestimmter gefährlicher Produkte zu untersagen). Gleichzeitig führt es auch zusätzliche Pflichten für die Hersteller ein. So etwa Informationspflichten gegenüber den Behörden, aber auch die Pflicht zum Vorhalten eines Rückrufmanagementsystems beim Vertrieb von Verbraucherprodukten.

Zunehmende Sensibilität ist im Zusammenhang mit produkthaftungsrechtlichen Fragen auch gegenüber den Vorgaben des **Strafrechts** erforderlich. Spätestens seit der bekannten „Lederspray-Entscheidung“[4] unterliegt es keinem Zweifel mehr, dass sich die Entscheidungsträger eines Unternehmens auch persönlich strafrechtlich für Produkthaftungsschäden zu verantworten haben. Und schließlich ist auch das **Versicherungsrecht** von großer Bedeutung in Produkthaftungs-Szenarien.

Neben den vorgenannten rechtlichen Fragen beinhaltet der proaktive Umgang mit Produkthaftungs-Themen aber natürlich noch eine weit größere Zahl von Faktoren im Unternehmen und verlangt zahlreiche eingespielte Prozesse quer durch das jeweilige Unternehmen.

Ein proaktives Herangehen an „Produkthaftung“ im Unternehmen soll hier wie folgt gegliedert werden:

- Einhaltung produktspezifischer Vorschriften
- Vermeidung von Risiken aus dem Produkt
- Vermeidung von Schäden aus riskanten Produkten
- Vermeidung von Kosten aus Schäden
- Vermeidung persönlicher Verantwortlichkeit

---

[3] Text erhältlich u.a. über die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, www.baua.de.

[4] BGH v. 6.7.1990 – 2 StR 549/89, NJW 1990, 2560.

2. Einhaltung produktspezifischer Vorschriften

In zahlreichen Vorschriften und Regelwerken sind detaillierte Vorgaben für die **Beschaffenheit** verschiedenster Produkte vorgegeben. Diese Vorgaben können unmittelbar verbindliche Wirkung besitzen, etwa in den zahlreichen und umfangreichen Verordnungen zum GPSG, aber auch in zahlreichen sonstigen Einzelverordnungen und Nebengesetzen[5]. Die Feststellung, welche Regularien für ein bestimmtes Produkt jeweils gelten, ist einem externen Juristen oftmals nahezu unmöglich. Hier stehen technische Fragen sowie Besonderheiten einzelner Produktgattungen im Vordergrund, die meist nur von erfahrenen Inhouse-Beratern oder Branchenvertretern abschließend überblickt werden können. Neben verbindlichen (gesetzlichen) Vorgaben für die Beschaffenheit von Produkten sind auch „freiwillige" Regelwerke wie DIN-Normen, Verbandsempfehlungen etc. von Bedeutung. Auch wenn diese keine direkte Zwangswirkung auf den Hersteller eines Produkts besitzen, können sie indirekt doch größte Bedeutung erfahren. Ein Produkt das nicht den vorgeschlagenen Sicherheitsstandard solcher Empfehlungen oder Normenkataloge aufweist, wird im Streitfalle nicht die erforderliche Sicherheit zugesprochen bekommen. Gleichzeitig kann das Abweichen von derartigen Standards in verschiedenen Konstellationen auch zum Verlust des Versicherungsschutzes führen.

Weiterhin sind auch Vorgaben für die vom Hersteller einzuhaltenden **Prozesse** zu beachten. Diese können Entwicklung und Erprobung der Produkte regeln. Besonders deutlich wird dies etwa im Arzneimittelzulassungsverfahren, wo detaillierteste Vorschriften die Prozesse im Vorfeld des Inverkehrbringens dieser Produktgattung regeln. Ähnliche Beispiele sind in anderen sehr sicherheitskritischen Produktbereichen zu finden (z. B. Flugzeugbau, Schienenverkehr, Nukleartechnik etc.). Auch hier ist neben direkt anwendbaren Gesetzen und Verordnungen die Bedeutung von Standards, Normen und Verbandsempfehlungen nicht zu unterschätzen.

Vorgaben für Prozesse können sich auch auf Sicherheitsvorkehrungen beziehen; etwa oblag dem Arzneimittelgroßhandel bereits vor Erlass des GPSG eine Rechtspflicht zum Vorhalten eines Rückrufmanagementsystems.

---

5 Vgl. die Auflistung des Bundesministeriums für Arbeit und Soziales, www.bmas.de, „Arbeitsschutz", „Gesetze".

3. Vermeidung von Risiken aus dem Produkt

Hersteller, Lieferanten, teils aber auch Importeure[6] sind sowohl zivilrechtlich als auch nach GPSG verpflichtet, nur solche Produkte in den Verkehr zu bringen, die die vom Benutzer berechtigterweise zu erwartende Sicherheit aufweisen. Die hierfür erforderlichen Prozesse umfassen Entwicklung, Beschaffung, Produktion und Instruktion.

Entwicklung: Proaktiv sollte ein Hersteller Qualität und Sicherheit stets bereits in sein Produkt hinein entwickeln. Entscheidend ist, welche Sicherheit der Benutzer berechtigterweise erwarten darf. Auch wenn insoweit aktuell keine „amerikanischen Verhältnisse" drohen, ist doch stets auch ein zu erwartender Fehlgebrauch[7] der Produkte zu berücksichtigen. Die sorgfältige Entwicklung sollte dabei nicht nur als Durchgangsstation hin zur Herstellung sicherer Produkte verstanden werden. Sie ist auch als Kriterium an sich zu verstehen – und sorgfältig zu dokumentieren. Dies kann Bedeutung erlangen, um etwa im Schadensfall demonstrieren zu können, dass ein bestimmtes Risiko im Zeitpunkt der Entwicklung des Produkts noch nicht erkennbar war (z. B. Handy-Strahlung?). Weiterhin ist dies etwa für den Erhalt des Versicherungsschutzes zentral. In nahezu allen Rückruf-Policen ist die sogenannte „Experimentierklausel" enthalten. Danach besteht Versicherungsschutz nur dann, wenn das betreffende Produkt nach dem Stand von Wissenschaft und Technik entwickelt und erprobt wurde und nicht etwa unter dem Fangnetz einer Versicherungs-Police voreilig in den Markt gedrückt wurde.

Beschaffung: Jeder Hersteller ist unter dem Gesichtspunkt der Produzentenhaftung verpflichtet, seine eigenen Vorlieferanten sorgfältig auszuwählen, zu überprüfen (auditieren?) und fortlaufend zu überwachen. Auch Versäumnisse in diesem Bereich können anderenfalls zu Schadensersatzansprüchen gegen den Hersteller führen.

Produktion: Naturgemäß ist eine lückenlose Qualitätssicherung während des Fertigungsprozesses zur Vermeidung von Produkthaftungsansprüchen unabdingbar. Nur mit einer derart dokumentierten Produktion ist es überhaupt möglich, der Haftung für „Ausreißer", d.h. unverschuldeten und unvermeidbaren Einzelfällen,[8] entgehen zu können. Zugegebenermaßen gelingt dies aber selbst dann nur in Einzelfällen.

Instruktion: Die umfassende und sorgfältige Instruktion der Benutzer eines Produkts über mögliche Risiken hieraus ist von großer Bedeutung. Allerdings kann auch sie nicht die gefährliche Konstruktion eines Produkts ausgleichen. Produkte müssen stets so konstruiert sein, dass sie im größtmöglichen Umfang Risiken von vornherein vermeiden. Der bloße Warnhinweis auf konstruktiv vermeidbare Risiken führt im Regelfall nicht zu einer Enthaftung des

---

6 Vgl. § 4 ProdHaftG; aber auch BGH v. 28.3.2006 – VI ZR 46/05, NJW 2006, 1589.

7 BGH v. 12.11.1991 – VI ZR 7/91, BGHZ 116, 60, 65.

8 Vgl. *Palandt/Sprau*, 67. Aufl. 2008, § 823 BGB, Rn. 169.

Herstellers.[9] Richtige Instruktion klärt darüber auf, (i) welches Verhalten gefährlich ist, (ii) was hierdurch passieren kann und (iii) welche Schäden dem Nutzer daraus drohen. Wichtig ist, dass der Hersteller den Erhalt dieser Hinweise beim Kunden im Streitfall auch nachweisen kann. Die Hinweise müssen jeweils in der betreffenden Landessprache erfolgen.[10] Bei schwerwiegenden Risiken müssen diese auch am Produkt selbst angebracht sein und nicht lediglich in einer beigefügten Bedienungs- oder Betriebsanleitung. Oft sind hier auch Aufkleber mit Piktogrammen etc. nach Maßgabe einschlägiger Vorschriften und Standards zu deren Gestaltung erforderlich. Zur Vermeidung von Gewährleistungsansprüchen sollte dabei auch auf Schäden hingewiesen werden, die zwar nicht dem Nutzer, aber dem jeweiligen Produkt drohen, wenn es in bestimmter Weise eingesetzt wird.

4. Vermeidung von Schäden aus riskanten Produkten

Produktbeobachtung: Nach den Grundsätzen der Produzentenhaftung ist der Hersteller eines Produkts auch nach Inverkehrbringen des Produkts verpflichtet, sein Produkt „im Auge zu behalten“. Dies gilt nach der bekannt gewordenen „Honda-Entscheidung“[11] nicht nur für das eigene Produkt, sondern auch für typischerweise damit gemeinsam verwendete Produkte Dritter (z. B. Accessoires, Zubehör etc.). Neben dieser Rechtspflicht ist es auch zur Vermeidung von teuren Schäden bzw. persönlicher Verantwortlichkeit ratsam, in jedem Unternehmen ein entsprechendes Beschwerdemonitoring einzurichten. Viele Schadensfälle wären vermeidbar gewesen, hätten die betroffenen Unternehmen ihren Kunden besser zugehört. Nicht nur ist es der Kundenbindung und dem Image eines Unternehmens abträglich, wenn dieses erst lange nach Auftreten entsprechender Diskussionsforen im Internet auf eine Produktkrise reagiert. Es kann darüber hinaus auch strafrechtliche Folgen haben, wenn ein Unternehmen erkennbare Risiken nicht oder zu spät beseitigt. Obendrein droht auch hier wieder der Verlust des Versicherungsschutzes, wenn ein Unternehmen Produkte unverändert auf den Markt liefert, während gleichzeitig bereits Erkenntnisse vorhanden waren, dass hier Sicherheitsrisiken bestehen können.

Die Installation eines schlüssigen Beschwerdemonitorings beinhaltet einige zu beachtende Kriterien, etwa zur Besetzung eines entsprechenden Gremiums, der Kriterien zur Auswertung erhaltener Informationen, Entscheidungs- und Eskalationskriterien etc. Neben einigen wenigen rechtlichen Fragen sind hier in erster Linie organisatorische Fragen entscheidend.

---

9 Produkthaftungshandbuch/*Foerste*, § 24 Rn. 97.

10 ebd., Rn. 208.

11 BGH v. 9.12.1986 – VI ZR 65/86, NJW 1987, 1009, 1010 f.

Rückrufmanagement: Die proaktive Installation eines Rückrufmanagements ist für eine große Zahl von Unternehmen bereits heute gesetzliche Rechtspflicht. Dies gilt insbesondere für Hersteller von Verbraucherprodukten im Sinne des GPSG.[12] Auch für alle anderen Hersteller von Produkten ist es jedoch im eigenen Interesse sehr ratsam, um nicht im Falle einer Produktkrise die Handlungsfähigkeit zu verlieren, sondern gegenüber Anspruchstellern, Presse, Behörden und anderen gewappnet zu sein. Kriterien die hier in noch stärkerem Maße als beim Beschwerdemonitoring zu berücksichtigen sind, sind die Zusammensetzung eines entsprechenden Gremiums, Personen, Kontaktdetails, Stellvertretungsregelungen etc.; Definition der Entscheidungskriterien; Kanäle der Informationsbeschaffung intern und extern (z. B. technische Analysefähigkeit, Rückverfolgbarkeit, Vertriebskanäle etc.); Kommunikationsregeln; Einbindung von Behörden; Pressearbeit, Rechtsberatung; Regeln zur Dokumentation der Entscheidungsfindung im Krisenfall etc.

Am Ende muss hier eine fundierte Entscheidung über einen möglichen Rückruf oder einen Warnhinweis stehen, diese rasch und effizient umgesetzt werden, gleichzeitig die Anspruchswahrung gegenüber Vorlieferanten und Versicherung gewahrt sein, dabei aber möglichen Ansprüchen Geschädigter nicht unnötig Tür und Tor geöffnet werden.

5. Vermeidung von Kosten aus Schäden

Vertragliche Haftungsbegrenzung im Verkauf: vertragliche Haftungsbeschränkungen entfalten nur Wirkung gegenüber dem Vertragspartner. Erleidet ein außenstehender Dritter aufgrund eines Produktfehlers einen Schaden und kann er aufgrund dessen von dem Hersteller Schadensersatz nach Deliktsrecht bzw. dem Produkthaftungsgesetz verlangen, spielen hierbei Haftungsbegrenzungen, die der Hersteller mit seinem Vertragspartner vereinbart hat, keine Rolle – der Dritte muss sich diese nicht entgegenhalten lassen.

Für den Hersteller eines Produkts ist die zivilrechtlich vorgesehene Haftung so klar wie ungünstig. Bei einem Produktfehler wird nicht nur Mangelbeseitigung geschuldet, sondern darüber hinaus auch der Höhe nach unbegrenzt auf den Ersatz sämtlicher Schäden einschließlich entgangenen Gewinns gehaftet. Dies resultiert daraus, dass der Hersteller – anders als der Händler – den Produktfehler regelmäßig verursacht hat und damit bei ihm das für die Verpflichtung zum Schadensersatz erforderliche Verschulden vorliegt.

Im Interesse eines effektiven Risk Managements sollte daher nach Möglichkeit die gesetzlich vorgesehene Haftung aus Gewährleistung vertraglich eingegrenzt werden. Ideal sind hier natürlich zunächst **individualvertragliche Haftungsbeschränkungen**, z. B.

---

[12] Vgl. § 5 Abs. 1 Nr. 1 lit.c) GPSG.

- Haftung auf Schadensersatz nur bei Vorsatz und grober Fahrlässigkeit (auch individualvertraglich kann die Haftung für den eigenen Vorsatz nicht ausgeschlossen werden, § 276 Abs. 3 BGB. Gleiches gilt für die zwingende Haftung eines Herstellers nach dem Produkthaftungsgesetz.)
- Haftung nur für Schäden am Produkt selbst/ keine Haftung auf entgangenen Gewinn
- Verkürzung der gesetzlich vorgesehenen Gewährleistungsfristen

Derartige Vereinbarungen bieten sich vor allem bei größeren Projekten mit hohem Haftungsrisiko an.

Im Übrigen sollte bei Vertragsschluss auf die eigenen **allgemeinen Verkaufsbedingungen** mit passenden Haftungsbeschränkungen verwiesen werden. Hierbei muss man sich jedoch über folgendes im klaren sein:

- In AGB sind Haftungsbeschränkungen nur in weit geringerem Rahmen zulässig als bei Individualvereinbarungen. Unzulässig sind Haftungsbeschränkungen bei
  - bei Verletzung von Leben, Körper und Gesundheit, § 309 Nr. 7a BGB[13]
  - grob fahrlässiger Pflichtverletzung durch den AGB-Verwender, vorsätzlich oder grob fahrlässige Pflichtverletzung des gesetzlichen Vertreters oder Erfüllungsgehilfen, § 309 Nr. 7b BGB
  - auch bei einfacher Fahrlässigkeit nur sehr eingeschränkt bei der Verletzung einer sog. Kardinalpflicht[14] = Pflicht, deren ordnungsgemäße Erfüllung die Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Vertragspartner vertraut und regelmäßig vertrauen darf.
  - Soweit der Kunde bei Vertragsschluss auf seine allgemeinen Einkaufsbedingungen mit für ihn günstigen Haftungsregelungen verweist, finden die sich widersprechenden AGB keine Anwendung und es bleibt damit bei der für den Verkäufer ungünstigen gesetzlichen Regelung.[15]

Befindet sich der Kunde in einer starken Verhandlungsposition, werden von ihm regelmäßig weder die AGB des Lieferanten, geschweige denn die vorstehenden individualvertraglichen Haftungsbeschränkungen akzeptiert. So ist es im Automotive-Bereich vielmehr üblich, dass von Seiten des OEM gegenüber seinen Zulieferern auf Klauseln bestanden wird, die das Haftungsrisiko sogar noch über das gesetzliche Maß hinaus ausweiten (z. B. Verlängerung der Gewährleistungsfristen von 24 auf bis zu 60 Monaten oder aber Möglichkeit der Durchführung eines Produktrückrufs auf Kosten des Zulieferers nach freiem Ermessen). Hier bietet sich eine andere Möglichkeit an, das eigene Haftungsrisiko sachgerecht zu begrenzen, nämlich die **Risikominimierung durch sachgerechte Leistungsbeschreibung.** Ein Produktfehler, der zu einer Haftung führen kann, liegt grundsätzlich nur dann vor, wenn das gelieferte

---

13 Dies gilt auch bei Verkürzung der Verjährungsfristen; BGH v. 15.11.2006 – VIII ZR 3/06, NJW 2007, 674.

14 Vgl. z. B. BGH v. 20.7.2005 – VIII ZR 121/04, NJW-RR 2005, 1496 ff.

15 z. B. BGH v. 23.1.1991 – VIII ZR 122/90, NJW 1991, 1606.

Produkt von der vertraglich vereinbarten Beschaffenheit abweicht.[16] Eine effektive Risikominimierung kann der Hersteller gegenüber dem Kunden also auch schon dadurch erreichen, dass er bei Vertragsschluss sachgerecht bzw. zurückhaltend/ vorsichtig festlegt

- was sein Produkt kann und was es nicht kann
- unter welchen Bedingungen sein Produkt die angegebene Leistung erbringt
- welche äußeren Einflüsse/sonstigen Faktoren negativen Einfluss auf das Produkt haben.

Einschränkungen in dieser Hinsicht stoßen erfahrungsgemäß auch bei einem verhandlungsstarken Gegenüber auf deutlich mehr Verständnis als der Wunsch nach haftungsbeschränkenden Klauseln.

Vertragliche Regresswahrung im Einkauf: Die allgemeinen Einkaufsbedingungen müssen das im Verkauf übernommene Risiko widerspiegeln. Der haftungsrechtliche „Worst case" für den Hersteller eines Produkts ist es, dass er gegenüber dem Kunden aufgrund der Verantwortlichkeit für das Endprodukt für einen Fehler einzustehen hat, der durch ein Zulieferteil verursacht wurde, er selbst aber bei dem Zulieferer keinen Regress nehmen kann. Im Rahmen des Einkaufs sollte daher sichergestellt werden, dass die Haftung der eigenen Zulieferer nicht hinter dem zurückbleibt, was man selbst dem Kunden gegenüber als Haftung übernommen hat. Dies macht eine Abstimmung zwischen Ein- und Verkauf erforderlich. Muss dem Kunden beispielsweise eine Verjährungsfrist von 48 Monaten für Sachmängel ab Ablieferung der Ware beim Kunden gewährt werden, so sollte darauf gedrängt werden, dass die Verjährungsfrist für den Zulieferer ebenfalls nicht vorher endet.

Vorsicht: Im Einzelfall ist eine lückenlose Absicherung wichtig. Es wäre im vorgenannten Beispiel nicht ausreichend, selbst wiederum eine Verjährungsfrist von 48 Monaten ab Ablieferung durch den Zulieferer zu vereinbaren. Zwischen Anlieferung des Zulieferteils und Ablieferung des Endprodukts liegt häufig ein nicht unerheblicher Zeitraum. Dies gilt oft selbst bei just-in-time Belieferung. Die Verjährungsfrist beginnt also für den Zulieferer gegenüber dem Hersteller früher als die Frist für den Hersteller gegenüber dem Endkunden.

Mögliche Vorgehensweise: Der Zulieferer wird bei Vertragsschluss dazu verpflichtet, die Einkaufsbedingungen des Endkunden zu akzeptieren und in dem gleichen Umfang zu haften, wie der Hersteller gegenüber dem Endkunden verantwortlich ist.

Soweit günstigere Individualvereinbarungen nicht durchsetzbar oder eine detaillierte Verhandlung der Konditionen (z. B. im Hinblick auf ein begrenztes Auftragsvolumen) nicht angebracht ist, sollte streng auf eine **wirksame Einbeziehung der eigenen allgemeinen Einkaufsbedingungen** geachtet werden – dies allein schon deshalb, damit nicht ansonsten die allgemeinen Verkaufsbedingungen des Vertragspartners zur Anwendung kommen.

Vorsicht: Im inländischen Geschäftsverkehr zwischen Unternehmern reicht es für die wirksame Einbeziehung der allgemeinen Geschäftsbedingungen in das Angebot aus, dass auf diese allgemein im Bestellschreiben verwiesen wird und die Gegenseite die Möglichkeit der

---

[16] § 434 Abs. 1 BGB.

Kenntnisnahme hat (z. B. durch Anfrage beim Vertragspartner oder durch Download von der Homepage des Bestellers).[17] Im grenzüberschreitenden Rechtsverkehr ist dies anders. Hier müssen dem Empfänger die AGB übersandt oder anderweitig zugänglich gemacht werden – es besteht also eine „Übermittlungspflicht" des Verwenders statt einer „Anforderungsobliegenheit" des Empfängers.[18] Zudem müssen die AGB in der Vertragssprache übermittelt werden.[19] Wird also zwischen den Parteien in englischer Sprache korrespondiert, reicht es nicht aus, die deutschsprachigen Einkaufsbedingungen dem Bestellschreiben beizufügen.

„To do's" zur Sicherstellung der richtigen Vorgehensweise in der Praxis – „Prozessqualität sichert Produktqualität":

Die Umsetzung der vorgenannten Punkte obliegt in der Praxis den Mitarbeitern der Ein- und Verkaufsabteilung. Diese sollten entsprechend geschult und für mögliche Probleme in rechtlicher Hinsicht sensibilisiert werden.

Im Hinblick darauf, dass gerade die Rechtsprechung zu allgemeinen Geschäftsbedingungen sehr komplex und immer noch im Fluss ist, ist es zudem ratsam, die eigenen AGB in regelmäßigen Abständen auf Änderungsbedarf hin überprüfen zu lassen. Im Übrigen kann es sich auch anbieten, interne Regularien aufzustellen die festlegen, welches Haftungsrisiko bei Vertragsschluss akzeptiert werden darf und welches nicht – bzw. der Genehmigung durch die Geschäftsführung bedarf.

Die Auswahl geeigneten **Versicherungsschutzes,** zugeschnitten auf die Produkte und die Vertriebswege des jeweiligen Unternehmens, sollte mit fachkundiger Beratung erfolgen. Hier sollten stets versierte Versicherungsmakler mit herangezogen werden. Die verschiedenen Möglichkeiten des Versicherungsschutzes (z. B. First Party/Third Party Recall) haben schon des Öfteren im Schadensfall für Überraschungen gesorgt. Gleichzeitig muss sichergestellt sein, dass der vorgehaltene Versicherungsschutz auch dem entspricht, wozu sich Lieferanten gegenüber ihren Kunden oft vertraglich verpflichten mussten.

Faktische Haftungsabwehr/faktische Regresswahrung Einige Punkte, die in diesem Zusammenhang unbedingt beachtet werden müssen: Wichtig ist die Rückverfolgbarkeit schadhafter Teile, Chargen, Lieferlose sowohl im Verhältnis zu Vorlieferanten als auch gegenüber Kunden. Die rechtzeitige Mängelrüge im Sinne von § 377 HGB muss unbedingt eingehalten werden. Im Rückruffall muss in jedem Fall auch eine umfangreiche und dokumentierte Beweissicherung stattfinden. Gemeinsam mit den Rechtsberatern sollte geklärt werden, ob dies im Rahmen eines selbständigen Beweisverfahrens stattfinden soll. In jedem Falle Aufbewahrung getauschter Teile für möglichen späteren Regressprozess. Dokumentation angefallener Kosten für Rückruf oder andere Feldmaßnahmen aufgeteilt nach den Vorgaben rechtlicher Durchsetzbarkeit verschiedener Schadenspositionen.

---

[17] BGH v. 30.6.1976 – VIII ZR 267/75, NJW 1976, 1886; BGH v. 3.2.1982 – VIII ZR 316/80, NJW 1982, 1750.

[18] BGH v. 31.10.2001 – VIII ZR 60/01, NJW 2002, 370 ff.

[19] Hanseatisches Oberlandesgericht v. 1.6.1979 – 11 U 32/79, NJW 1980, 1232, 1233.

Bewusste Entscheidung über schriftliche Dokumentation im Krisenfalle unter Berücksichtigung eines möglichen Zugriffs von außen auf diese Dokumente (z. B. US-Pre-Trial-Discovery). Zahlungen stets nur unter Vorbehalt (Anerkenntnisverbot!).

6. Vermeidung persönlicher Verantwortlichkeit

Eine **zivilrechtliche Haftung** der handelnden Personen in einem Unternehmen gegenüber Dritten stellt grundsätzlich die Ausnahme dar. Dies gilt jedenfalls dann, wenn das Unternehmen als juristische Person (z. B. GmbH, AG) organisiert ist und die betreffenden Mitarbeiter und Entscheidungsträger ausdrücklich nicht im eigenen Namen, sondern für das Unternehmen handeln. Es ist das Wesen des Handelns für eine juristische Person, dass dessen Folgen nur das Unternehmen und nicht die handelnden Personen selbst treffen. Von diesem Grundsatz gibt es jedoch Ausnahmen („Piercing the corporate veil"):

Eine Haftung gegenüber außenstehenden Dritten kann etwa nach Deliktsrecht dann erfolgen, wenn der betreffende Entscheidungsträger durch sein Handeln – mag dies auch für das betroffene Unternehmen erfolgt sein – schuldhaft absolute Rechte Dritter verletzt.[20] Hierbei kann es sich um Eigentumsverletzungen, aber auch um die Verletzung von Leben oder Gesundheit handeln. Voraussetzung hierfür ist es jedoch, dass etwa ein Geschäftsführer durch sein Handeln sämtliche Tatbestandsvoraussetzungen einer unerlaubten Handlung (§ 823 BGB) in seiner Person verwirklicht. Eine persönliche Haftung nach Deliktsrecht kommt aber nach § 823 Absatz 2 BGB auch dann in Betracht, wenn der Geschäftsführer durch sein Handeln gegen eines der dort in Bezug genommenen Schutzgesetze verstößt. Dies ist insbesondere bei strafrechtlich relevantem Handeln der Fall (z. B. fahrlässige Körperverletzung oder Tötung durch Unterlassung). Desweiteren kann dies auch bei Verstößen gegen Produktsicherheitsrecht der Fall sein.[21] Andere Fallgruppen der persönlichen Haftung gegenüber Dritten, wie etwa der Inanspruchnahme besonderen persönlichen Vertrauens, spielen im Bereich der Produkthaftung üblicherweise keine Rolle.

Eine **zivilrechtliche Haftung** gegenüber der Gesellschaft kann dagegen auf Grundlage der gesetzlichen Vorschrift in § 43 GmbHG (für Geschäftsführer einer GmbH), von § 93 AktienG (für Vorstände einer AG) oder auf Grundlage des jeweiligen Anstellungsvertrages (für sonstige Mitarbeiter) vergleichsweise leichter erfolgen. Wenn hier auch stets die Besonderheiten des jeweiligen Einzelfalls zu berücksichtigen sind, ist doch das jeweilige Organ / der jeweilige Mitarbeiter der betroffenen Gesellschaft verpflichtet, gegenüber der Gesellschaft deren Interessen zu wahren und Schäden von der Gesellschaft abzuwenden. Hier mag es durchaus

---

20 BGH v. 5.12.1989 – VI ZR 335/88, BGHZ 109, 297, 302.

21 BGH v. 28.3.2006 – VI ZR 46/05, NJW 2006, 1589.

im Einzellfall Zielkonflikte geben, wenn es etwa darum geht, die oft nicht unbeträchtlichen Kosten eines Produktrückrufs gegenüber den im Worst Case deutlich höheren aber im Zeitpunkt der Entscheidungsfindung nur hypothetisch zu bewertenden Kosten eingetretener Schadensfälle gegeneinander abzuwägen. Allerdings dürfte hier im Zweifel die in jedem Fall bestehende Pflicht der Gesellschaft, sich rechtskonform zu verhalten, eine wichtige Entscheidungshilfe für die betroffenen Geschäftsführer, Vorstände oder Mitarbeiter sein.

Eine **strafrechtliche Verantwortlichkeit** der Entscheidungsträger eines Unternehmens muss spätestens seit der „Lederspray-Entscheidung" des Bundesgerichtshofs als ernst zu nehmende Gefahr betrachtet werden und kann nicht mehr als eher theoretische Problematik abgetan werden. Im Bereich der Produkthaftung drohen hier persönliche Verantwortlichkeiten im Bereich der fahrlässigen Körperverletzung oder Tötung durch Unterlassen. Dies kann etwa dann eintreten, wenn die Entscheidungsträger eines Unternehmens von einer ernstzunehmenden Gefahr für die Benutzer eines Produkts aus Sicherheitsmängeln wissen und dennoch untätig bleiben. Der Unterlassungsvorwurf kann dabei zweierlei Stoßrichtungen haben: (i) es unterlassen zu haben, das Produkt aus dem Verkehr zu nehmen und es in Kenntnis der Sicherheitsrisiken weiter hergestellt und vertrieben zu haben sowie (ii) es unterlassen zu haben, die bereits im Markt befindlichen Produkte zurückzurufen bzw. einen Warnhinweis an die Benutzer zu verbreiten.

Um sich sowohl hinsichtlich einer zivilrechtlichen Verantwortlichkeit, als auch hinsichtlich einer strafrechtlichen Verantwortlichkeit im Rahmen des Möglichen abzusichern, ist es von entscheidender Bedeutung, dass die Entscheidungsträger des Unternehmens ein stringentes System der **Delegation** einrichten. Im Bereich der Produkthaftung setzt dies schlüssige Prozesse für Entwicklung, Beschaffung, Produktion und Instruktion voraus; weiterhin aber auch für Produktbeobachtung und Rückrufmanagement. Um hier in den Genuss einer möglichen Enthaftung zu kommen, müssen diese Prozesse aber nicht nur theoretisch vorgegeben sein. Sie müssen vielmehr tatsächlich erfolgreich implementiert werden. Dies beinhaltet, dass die betroffenen Mitarbeiter sorgfältig ausgewählt werden, fortlaufend geschult aber auch kontrolliert werden.[22] Nur ein solches in sich geschlossenes System kann für das Management eines Unternehmens dazu führen, dass im Falle von dennoch auftretenden Schäden keine persönliche Verantwortlichkeit der Entscheidungsträger vorliegt.

Wichtig ist, dass etwa einzelne Mitglieder eines Geschäftsführungsgremiums sich nicht darauf berufen können, dass die Verantwortung gemäß der internen Geschäftsverteilung nicht in ihr Ressort fällt. Im Falle erkannter Risiken ist – wie auch bei anderen Compliance-Fragen – eine Verantwortlichkeit des Gesamtgremiums Geschäftsführung bzw. Vorstand anzunehmen.[23] Jedes einzelne Mitglied des Unternehmensmanagements muss daher die in seiner Macht stehenden Schritte zur Vermeidung von Schäden ergreifen, um einer persönlichen Verantwortlichkeit entgehen zu können.

---

[22] Vgl. *Schneider,* in: Scholz, GmbHG, 10. Aufl. 2007, § 43 Rn. 41.

[23] ebd., Rn. 39.

Due Diligence: Compliance bei M&A Transaktionen

Christofer Rudolf Mellert

Zusammenfassung

Im Rahmen der aktuellen Compliance Diskussion wird der Bereich der M&A – Transaktionen oftmals ausgespart. Dies geschieht – wie die nachfolgenden Ausführungen zeigen werden – zu Unrecht, haben doch die involvierten Parteien selbstverständlich auch bei der Durchführung derartiger Transaktionen sicherzustellen, dass nicht gegen geltendes Recht verstoßen wird.

Ein Bereich, in dem dies in besonderem Maße sicherzustellen ist, ist die so genannte Due Diligence, d. h. die Untersuchung des zu erwerbenden Unternehmens durch den Käufer[1] (teilweise auch bereits durch den Verkäufer in Form einer so genannten Vendor Due Diligence). Hintergrund einer solchen Due Diligence ist die Schaffung einer Basis für die Entscheidung über den Kauf. Damit ist eine Due Diligence zum einen dem Bereich der Sorgfaltspflichten der Geschäftsleitung (Vorstand, Aufsichtsrat und Geschäftsführung) des Käufers zuzuordnen. Für den Verkäufer stellt sich bei der Due Diligence hingegen die Frage, welche Informationen er ohne Verstoß gegen geltendes Recht oder gegen Vereinbarungen mit Dritten offen legen darf.

Auch in Bezug auf die Vertraulichkeit bei M&A – Transaktionen sollte ein Unternehmen über ein entsprechendes Compliance Management verfügen. M&A – Transaktionen unterliegen meist einer sehr hohen Vertraulichkeitsstufe. Bei den beteiligten Unternehmen ist in der Regel nur ein kleiner Personenkreis über die Transaktion und ihre Details informiert. Üblicherweise sind dies die Geschäftsleitung sowie Mitarbeiter der M&A – Abteilung, der Steuerabteilung, des Controlling und der Rechtsabteilung. Bei komplexeren Transaktionen sind diesem Personenkreis noch die externen Berater, d. h. im Allgemeinen Rechtsanwälte, Steuerberater, M&A – Berater etc. hinzuzurechnen. Hierbei gilt es zum einen, das nachteilige Durchsickern von Informationen aus verhandlungstaktischen Gründen zu vermeiden. Zum anderen kann Vertraulichkeit auch gesetzlich angeordnet sein, etwa in Bezug auf Insider –

1 *Werner,* GmbHR 2007, 678; Allgemein zur Due Diligence *Berens/Brauner*, Due Diligence bei Unternehmensakquisitionen, 4. Aufl. 2005.

Informationen bei börsennotierten Unternehmen.[2] Daneben werden häufig vertragliche Vertraulichkeitsverpflichtungen (mit oder ohne Vertragsstrafen) abgeschlossen, deren Bestimmungen es ebenfalls einzuhalten gilt.

1. Due Diligence als Bestandteil der unternehmerischen Sorgfalt

Die Geschäftsleitung des kaufinteressierten Unternehmens hat die Entscheidung zu treffen, ob das Zielunternehmen gekauft wird oder nicht und trägt insoweit für diese Entscheidung auch die Verantwortung. Vor diesem Hintergrund ist sicherzustellen, dass den gesetzlichen Vorgaben für solche Entscheidungen entsprochen wird, um u.a. eine persönliche Haftung der Geschäftsleiter zu verhindern.

Dem Vorstand einer AG steht bei Ausübung seiner Unternehmensleitungsfunktion bei unternehmerischen Entscheidungen ein weit reichender, gerichtlich nicht überprüfbarer Ermessensspielraum zu.[3] Ähnliches gilt für den Geschäftsführer einer GmbH, solange er sich nicht am Willen der Gesellschafter zu orientieren hat.[4]

Dieses unternehmerische Ermessen ist jedoch insoweit eingeschränkt, als dass der Geschäftsleiter seine Entscheidung nicht ins Blaue hinein treffen darf. Die Entscheidung ist vielmehr auf Basis ausreichender Informationen und Außerachtlassung sachfremder Erwägungen und Eigeninteressen zu treffen. Eine Pflichtverletzung liegt daher solange nicht vor, wie das Vorstands- / Geschäftsführungsmitglied bei seiner Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln.

Speziell für Unternehmenskäufe bedeutet dies, dass der Geschäftsleiter die Zielgesellschaft vor Erwerb mehr oder weniger umfassend zu prüfen hat, um sich ein Bild über diese zu verschaffen und etwaige Risiken zu erkennen. Übliches Verfahren für eine solche Prüfung ist heute die aus dem anglo-amerikanischen Rechtskreis stammende Due Diligence. Ob eine solche heute bereits kraft Verkehrssitte etabliert ist, so dass der Verzicht auf eine solche Prüfung im Zweifelsfall einen Sorgfaltsverstoß indiziert, ist umstritten.[5] Vereinzelte Gerichtsurteile lassen jedoch einen Trend der Rechtsprechung hin zu einer Haftungsverschärfung für die Geschäftsleitungsmitglieder insgesamt erkennen, was sich auch im Bereich der Due Diligen-

---

2 Zur Weitergabe von Insiderinformationen bei M & A – Transaktionen mit börsennotierten Aktiengesellschaften vgl. *Hasselbach,* NZG 2004, 1087 ff.

3 BGH v. 21.4.1997 – II ZR 175/95, BGHZ 135, 244 (253) [ARAG- Garmenbeck- Entscheidung].

4 *Lutter,* GmbHR 2000, 301 (306).

5 *Werner*, GmbHR 2007, 678 (679) m.w.N. in Fn. 19.

ce auswirkt.[6] So lässt sich einem kürzlich ergangenen Urteil des OLG Oldenburg entnehmen, dass das Unterlassen einer Due Diligence beim Unternehmenskauf durch die Geschäftsführung des kaufenden Unternehmens eine Sorgfaltspflichtverletzung darstellen kann. Wörtlich heißt es im Leitsatz 2:

> *„Das dem Geschäftsführer bei unternehmerischen Entscheidungen zuzubilligende weite Ermessen ist beim Erwerb eines anderen Unternehmens (hier eines weiteren Klinikbetriebs) beschnitten, wenn die Grundlagen, Chancen und Risiken der Investitionsentscheidung nicht ausreichend aufgeklärt worden sind. Zumindest dann, wenn nicht ausreichende, gesicherte Erkenntnisse über das zu erwerbende Unternehmen vorhanden sind oder wenn vorhandene Informationen Unklarheiten aufweisen, wird eine umfassende Due Diligence durchzuführen sein. Wird dies unterlassen, kommt bei einer zu erheblichen Verlusten führenden Fehlinvestition eine Geschäftsführerhaftung in Betracht.“* [7]

Eine Pflicht zur Durchführung einer Due Diligence ist allerdings abhängig von der tatsächlichen Möglichkeit einer Durchführung. Eine umfassende Due Diligence kann etwa dann nicht durchgeführt werden, wenn das Management des Zielunternehmens die Herausgabe relevanter Informationen ganz oder teilweise verweigert (z. B. bei börsennotierten Unternehmen nicht unüblich). In einem solchen Fall kann dennoch die Entscheidung zum Erwerb des entsprechenden Unternehmens im Rahmen des unternehmerischen Ermessenspielraums liegen. Dann müssen etwaige Risiken aber durch weitreichende Garantien des Verkäufers abgedeckt werden. Ist selbst dies nicht möglich, kann eine Due Diligence auch dann entbehrlich sein, wenn etwaige Risiken bereits bei der Höhe des Kaufpreises berücksichtigt sind, d.h. der Kaufpreis entsprechend vermindert ist.

2. Grenzen der Zurverfügungstellung von Informationen in der Due Diligence

Im Rahmen der Durchführung einer Due Diligence stellen sich rechtliche Fragen jedoch auch auf Seiten des Verkäufers und des Zielunternehmens. Insofern geht es hier mehr um die Frage der Zulässigkeit der Zurverfügungstellung von Informationen,[8] als um etwaige Pflichten des Verkäufers, d.h. der Gesellschafter des zu verkaufenden Unternehmens selbst.

---

6 LG Frankfurt a.M. v. 7.10.1997 – 3/11 O 44/96, WM 1998, 1181 (1185).

7 OLG Oldenburg v. 22.06.2006 – 1 K 34/03, NZG 2007, 434 ff.

8 Einen guten Überblick hierzu bietet *Rittmeister,* NZG 2004, 1032 ff.

Grundsätzlich gilt für einen Geschäftsführer oder ein Mitglied des Vorstandes, dass vertrauliche Informationen, die das Unternehmen betreffen, Dritten nicht zugänglich gemacht werden dürfen, wenn dies dem Interesse des Unternehmens widerspricht.[9] Dies gilt im Prinzip auch bei einer Due Diligence. Jedenfalls in Fällen, in denen die Person des Gesellschafters eines Unternehmens irrelevant oder in Bezug auf den potentiellen Erwerber für das Zielunternehmen sogar nachteilig ist, dürfte daher der Geschäftsführer des Zielunternehmens grundsätzlich überhaupt keine vertraulichen Informationen im Rahmen einer Due Diligence zur Verfügung stellen.[10] Dies gilt insbesondere in Fällen, in denen der Erwerber ein Wettbewerber des kaufgegenständlichen Unternehmens ist.[11] Bei der GmbH lässt sich dieses Verbot jedoch im Allgemeinen durch eine Weisung der Gesellschafterversammlung aushebeln.[12] Ein Mehrheitsgesellschafter als Verkäufer kann daher das Management des Zielunternehmens zur Bereitstellung der Due Diligence Unterlagen zwingen, ohne dass die Geschäftsführer des Zielunternehmens hierbei eine Haftung trifft. Darüber hinaus hat aber auch jeder Gesellschafter, d. h. Mehrheits- oder Minderheitsgesellschafter, einer GmbH das Recht von der Geschäftsführung umfassend über die Geschäfte der Gesellschaft informiert zu werden.[13] Die Geschäftsführung ist daher insoweit verpflichtet, ihre Gesellschafter mit entsprechenden Informationen zu versorgen,[14] so dass ein Gesellschafter als Verkäufer sich auf diesem Wege Informationen beschaffen und diese dem Erwerber dann selbst zur Verfügung stellen könnte.

Bei einer Aktiengesellschaft ist dies jedoch grundsätzlich anders. Es besteht zum einen schon kein Weisungsrecht der Aktionäre bzw. der Hauptversammlung gegenüber dem Vorstand, d.h. es gilt die allgemeine Regel, dass vertrauliche Informationen nur weitergegeben werden dürfen, wenn dies im Interesse des Unternehmens liegt. Des Weiteren ist die Informationspflicht des Vorstands gegenüber Aktionären gesetzlich auf hauptversammlungsrelevante Themen beschränkt. Damit unterliegt es der unternehmerischen Entscheidung des Vorstands, ob und inwieweit er einem Aktionär oder dem Erwerber vertrauliche Informationen für eine Due Diligence zur Verfügung stellt. Hierbei hat er eine Abwägung der Interessen des Unternehmens gegen die des Aktionärs vorzunehmen.[15] In der Praxis wird dieses rechtliche Idealbild jedoch meist nicht gelebt, d. h. ein starker Hauptaktionär wird seinen Einfluss auf den Vorstand immer zu seinen Gunsten auszuüben wissen. Einen Sonderfall bildet der Paketverkauf von Aktien börsennotierter Unternehmen außerhalb der Börse. Dort findet meist nur eine

---

9 Für den Vorstand einer AG siehe *Thiel* in: Semler/ Volhard, Arbeitshandbuch für Unternehmensübernahmen Band 2, 2003, § 54 Rn. 41; für den GmbH- Geschäftsführer siehe *Dietzel* in: Semler/Volhard, Arbeitshandbuch für Unternehmensübernahmen Band 1, 2001, § 9 Rn. 78.

10 *Bremer*, GmbHR 2000, 176.

11 *Schiessl*, Münchener Handbuch des Gesellschaftsrechts Band 3, 2. Aufl. 2003, § 33 Rn. 20.

12 *Götze*, ZGR 1999, 202 (227).

13 Vgl. § 51 a GmbHG; *Schmiegelt* in: Beck´sches Handbuch der GmbH, 3. Aufl. 2002, § 3 Rn. 63.

14 *Koppensteiner,* in: Rowedder/ Schmidt- Leithoff, GmbHG, 4. Aufl. 2002, § 51 a Rn. 5: informationsverpflichtet ist insofern nur die Gesellschaft die dabei aber durch die Geschäftsführer vertreten wird.

15 *Richter,* in: Semler/Peltzer, Arbeitshandbuch für Vorstandsmitglieder, München 2005, § 4 Rn. 362; OLG Hamm v. 10.5.1995 – 8 U 59/94, AG 1995, 512 (514).

sehr eingeschränkte Due Diligence statt, da das börsennotierte Zielunternehmen bzw. dessen Organe aus insiderrechtlichen Gründen diverse Informationen nicht zur Verfügung stellen dürfen.[16]

Neben der Frage der Zulässigkeit der Herausgabe vertraulicher Informationen durch die Geschäftsleitung des Zielunternehmens ist in zweiter Linie zu prüfen, inwieweit der Verkäufer, d. h. der Gesellschafter bzw. Aktionär des Zielunternehmens selbst berechtigt ist, das Zielunternehmen betreffende vertrauliche Informationen an Dritte weiterzugeben. Er unterliegt ebenfalls einer Treuepflicht gegenüber der Zielgesellschaft, die allerdings weniger intensiv ausgeprägt ist als die Treuepflicht des Geschäftsführers bzw. Vorstandsmitglieds. Darüber hinaus ist bei der eher personalistisch geprägten GmbH der Gesellschafter grundsätzlich weitergehend zur Treue verpflichtet als der Aktionär einer als Publikumsgesellschaft ausgestalteten AG. Auch hier ist eine Abwägung vorzunehmen zwischen den Interessen der zu veräußernden Gesellschaft und ihres Gesellschafters bzw. Aktionärs.[17] Soweit eine echte Verkaufsabsicht des Aktionärs bzw. Gesellschafters besteht, dürfte jedoch üblicherweise die Treuepflicht eine Informationsweitergabe nicht untersagen.

Zu beachten ist jedenfalls, dass Informationen eines höheren Vertraulichkeitsgrades nicht gleich zu Beginn der Due Diligence zur Verfügung gestellt werden, sondern erst, wenn eine Kaufabsicht des Käufers hinreichend konkret ist und die Weitergabe dieser höchst vertraulichen Informationen eine notwendige Voraussetzung für den Kauf bildet.

3. Compliancebezogene Due Diligence?

Neben den klassischen Formen der Due Diligence (rechtliche, steuerliche, finanzielle, technische, umweltbezogene etc.) etabliert sich mehr und mehr eine rein compliancebezogene Due Diligence (wobei dies eher als Bestandteil einer rechtlichen, organizational oder IT – Due Diligence stattfinden wird). Ein Käuferunternehmen, bei dem bereits ein funktionierendes Compliance Management besteht, muss sich im Vorfeld eines Kaufes auch ein Bild darüber machen, inwieweit ein solches Compliance Management auch bei dem zu erwerbenden Unternehmen besteht bzw. welcher Aufwand zur Einführung eines Systems betrieben werden muss. Besteht bereits eine Compliance Organisation, so ist zu untersuchen, inwieweit sich diese in die eigene integrieren lässt. Ist dies nicht möglich bzw. besteht noch keine Compliance Organisation, so muss man sich über den Aufwand ein Bild machen, der erforderlich ist, um die eigene Compliance Organisation beim Zielunternehmen einzuführen.

---

16 Vgl. hierzu *Körber*, NZG 2002, 263 (267).

17 Zur Geheimhaltungspflicht von Gesellschaftern vgl. *Ziegler,* DStR 2000, 249 ff.

Bestehen beim Zielunternehmen keine Compliance Organisation oder ähnliche Systeme, so können hieraus (müssen aber nicht) auch Schlüsse in Bezug auf etwaige Risken gezogen werden. Dies dürfte jedoch sehr von der Branche des Zielunternehmens abhängen.

4. Geheimhaltung

Wie eingangs bereits beschrieben, ist bei M & A –Transaktionen unbedingt absolute Vertraulichkeit zu gewährleisten. Dies gilt zum einen im Hinblick auf das Verhindern des Durchsickerns von Informationen und damit zur Stärkung der eigenen Verhandlungsmacht. Zum anderen sind insbesondere bei börsennotierten Unternehmen nachteilige Folgen mit der Weitergabe von vertraulichen Informationen verbunden.

Darüber hinaus gibt es vertrauliche Informationen, die dem Käufer vor Abschluss des Kaufvertrages überhaupt nicht zur Verfügung gestellt werden können. Dies sind in erster Linie Informationen, die aufgrund einer Vertraulichkeitsvereinbarung mit Dritten (z. B. Vertragspartnern) nicht weitergegeben werden dürfen, ohne gleichzeitig Vertragsstrafen oder Kündigungsrechte für den Dritten auszulösen. Insbesondere wenn es sich bei dem Erwerber um einen Wettbewerber handelt, werden solche Informationen oftmals auch erst nach Vertragsabschluss offengelegt, soweit diese Informationen einen wesentlichen nachteiligen Effekt für das Zielunternehmen hätten, falls es nicht zu einem Vertragsabschluss kommt (z. B. Preiskalkulationen in einer Wettbewerbssituation u. ä.).[18]

In größeren Unternehmen sowie bei auf M & A – Transaktionen spezialisierten Beratern ist es daher üblich, Verhaltensrichtlinien für M & A – Transaktionen an die Mitarbeiter zu verteilen. Solche Regeln gehen oft einher mit IT – Sicherheit und Compliance, da ohne IT – Support eine Transaktion heutzutage kaum noch denkbar ist. Insbesondere der E-Mail-Verkehr mit vertraulichen Informationen sollte möglichst eingedämmt bzw. kanalisiert werden. Zur Verbesserung der Geheimhaltung eignen sich z. B. virtuelle webbasierte Plattformen (z. B. Dealroom) in die sämtliche relevanten Informationen und Dokumente eingestellt werden und auf die nur ein ausgewählter Personenkreis Zugriff hat.

---

18 *Semler,* in: Hölters, Handbuch des Unternehmens- und Beteiligungskaufs, 6. Aufl. 2005, Teil VII Rn. 51.

5. Fazit

Wie die vorausgehenden Ausführungen zeigen, ist ein funktionierendes Compliance-Management aufgrund der einzuhaltenden Vorschriften und damit verbunden Risiken vom Anfang bis zum Ende eines M & A – Transaktionsprozesses höchst relevant. Ist ein Unternehmen erworben, muss sichergestellt werden, dass die etwa vorhandenen verschiedenen Compliance Systeme kompatibel sind oder es muss das eigene Compliance System bei dem erworbenen Unternehmen eingeführt werden. Dies erfordert eine genaue und zeitnahe Vorbereitung. Der Compliance Officer ist frühzeitig in den Transaktionsprozess einzubinden, damit eine reibungslose Integration des erworbenen Unternehmens auch aus Compliance Gesichtspunkten möglich ist.

Compliance in der Außenwirtschaft: Exportkontrolle

Henning Lustermann / Markus Witte

Zusammenfassung

Die Bundesrepublik Deutschland nimmt für sich gerne den Titel des Exportweltmeisters in Anspruch. Gerade Exporte können jedoch für die Geschäftsleitung eines Unternehmens mit hohen – auch persönlichen – Risiken verbunden sein. Nicht nur die klassischen Rüstungsgüter, sondern auch scheinbar harmlose zivile Technologien können in den falschen Händen – die man wiederum zunächst einmal als solche erkennen muss – erhebliche Auswirkungen nicht nur auf die Sicherheitsinteressen der Bundesrepublik Deutschland, sondern auch auf ihr außenpolitisches Ansehen haben. Dementsprechend streng sind die drohenden Sanktionen für die Verantwortlichen, wenn gegen Vorschriften des Außenwirtschaftsrechts verstoßen wird.

Jedes exportierende Unternehmen muss sich daher mit den grundlegenden Regelungen des Exportkontrollrechts auseinandersetzen und die erforderlichen Maßnahmen treffen, um Verstöße nach Möglichkeit auszuschließen. Dies gilt nicht nur für einige wenige Mitarbeiter, sondern auch insbesondere für die Unternehmensleitung. Denn wer die politische Vorgabe „**Exportkontrolle sollte Chefsache sein, und der Chef muss Vorbild sein**“[1] ignoriert, riskiert bei Nachlässigkeiten seiner Mitarbeiter nicht nur erhebliche Imageverluste für das Unternehmen, sondern schlimmstenfalls sogar mehrjährige Haftstrafen.

Der Beitrag stellt zunächst im Überblick die wichtigsten Beschränkungen des grundsätzlich freien Außenhandels (§ 1 Außenwirtschaftsgesetz) dar. Es folgen einige Ausführungen zum Ablauf des Genehmigungsverfahrens beim zuständigen Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) und schließlich eine Übersicht über die drohenden Sanktionen sowie die wichtigsten Compliance-Maßnahmen im Rahmen des Außenwirtschaftsrechts.

1 Bundesamt für Wirtschaft und Ausfuhrkontrolle (Hrsg.), Praxis der Exportkontrolle, S. 25.

1. Beschränkungen des Außenwirtschaftsverkehrs

Die Kontrollmechanismen des Außenwirtschaftsrechts beruhen zumindest in gewissem Umfang auf internationalen Übereinkommen, insbesondere den so genannten Exportkontrollregimen (Wassenaar, NSG, Australische Gruppe, MTCR). Insoweit bot es sich an, das Exportkontrollrecht zumindest teilweise auf europäischer Ebene einheitlich zu regeln. Wichtigstes Regelwerk in diesem Zusammenhang ist die so genannte EG Dual-use-Verordnung (EG Dual-use-VO), die in allen Mitgliedstaaten unmittelbar anwendbar ist. Eine vollständige Harmonisierung scheiterte allerdings an den Vorbehalten der einzelnen Mitgliedstaaten. Daher werden die europarechtlichen Regelungen weiterhin durch nationales Recht ergänzt, in Deutschland insbesondere durch das Außenwirtschaftsgesetz (AWG) und die Außenwirtschaftsverordnung (AWV).[2]

Im Folgenden werden nun die einzelnen Tätigkeiten und Bereiche, für die exportkontrollrechtliche Beschränkungen bestehen, näher dargestellt.

1.1 Ausfuhr

Unter einer **Ausfuhr** versteht das Außenwirtschaftsrecht den Export von Gütern in einen Staat außerhalb der Europäischen Union. Der Begriff **Güter** wiederum umfasst im europäischen ebenso wie auch im deutschen Recht

- Waren
- Software und
- Technologie

Unter Technologie versteht man sowohl verkörpertes technisches Wissen in Form von Unterlagen wie Handbüchern, Blaupausen etc. als auch das technische Wissen als solches, das mündlich oder in sonstiger Weise als so genannte technische Unterstützung an Dritte weitergegeben werden kann.[3]

Die Einbeziehung immaterieller Güter wie Software und Technologie in den Bereich der Ausfuhrkontrolle führt auch dazu, dass nicht nur die körperliche Versendung von Waren als

---

2 Eingehend zur Entwicklung des Exportkontrollrechts in Europa *Simonsen,* in: Wolffgang / Simonsen (Hrsg.), AWR-Kommentar, Kommentar für das gesamte Außenwirtschaftsrecht, Band 1, Loseblatt, Stand: August 2007, Einführung zur Dual-use-VO.

3 *Tervooren / Mrozek,* in: Wolffgang / Simonsen (Hrsg.), a.a.O., Art. 2 Dual-use-VO Rn. 7.

Ausfuhr gilt, sondern ggf. auch die elektronische Übertragung von Daten per E-Mail oder die Bereitstellung zum Download.[4]

Bei Ausfuhren gilt es nacheinander die **folgenden drei Prüfungsschritte** durchzugehen:

1.2 Embargos

Unter einem **Embargo** versteht man grundsätzlich ein auf Beschlüssen internationaler Organisationen beruhendes Handelsverbot. Dies sind in Europa insbesondere Beschlüsse des UN-Sicherheitsrates sowie Beschlüsse der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) und Beschlüsse der Europäischen Union im Rahmen der gemeinsamen Außen- und Sicherheitspolitik (GASP).[5]

Die USA kennen allerdings auch unilaterale Embargos wie etwa das gegen Kuba. Eine Verletzung dieser Embargobestimmungen wird in Europa nicht geahndet und teilweise ist ihre Befolgung (wie im Fall des Kuba-Embargos) sogar gesetzlich verboten.[6] Die Nichtbeachtung von US-Embargos kann allerdings negative Auswirkungen auf das USA-Geschäft eines Unternehmens haben.

Embargos lassen sich zum einen nach ihrem **Anknüpfungspunkt** und zum anderen nach ihrem **Umfang** unterscheiden.

Anknüpfungspunkt kann grundsätzlich entweder

- das **Bestimmungsland** oder
- die Person des **Geschäftspartners**

sein. Ferner existieren auch Mischformen wie etwa derzeit die Sanktionen gegen bestimmte weißrussische Funktionäre oder bestimmte iranische Unternehmen und Personen.

Personenbezogene Embargobestimmungen kommen insbesondere im Rahmen der Bekämpfung des internationalen Terrorismus zum Einsatz. So existieren zwei Listen der EU (die wiederum auf Listen des UN-Sicherheitsrates basieren), auf denen Personen und Unternehmen aufgeführt sind, die dem Umfeld der Taliban oder des Terrornetzwerks „Al Kaida“ einerseits oder dem Umfeld sonstiger internationaler Terrororganisationen andererseits zugerechnet werden. Auf diesen Listen befinden sich auch Personen und Unternehmen aus Deutschland und anderen europäischen Staaten.

---

4 *Tervooren / Mrozek*, a.a.O., Art. 2 Dual-use-VO Rn. 21 ff.

5 Bundesamt für Wirtschaft und Ausfuhrkontrolle (Hrsg.), HADDEX Handbuch der deutschen Exportkontrolle, Band 1, Loseblatt, Stand: Juli 2007, Rn. 83 ff.

6 Vgl. insoweit die Verordnung (EG) Nr. 2271/96 des Rates vom 22. November 1996 zum Schutz vor den Auswirkungen der extraterritorialen Anwendung von einem Drittland erlassener Rechtsakte sowie von darauf beruhenden oder sich daraus ergebenden Maßnahmen.

Praxishinweis

> Eine Kontrolle im Hinblick auf die so genannten Terrorlisten kann in größerem Umfang nur EDV-gestützt erfolgen. Nur so ist aufgrund der häufigen Änderungen auch eine regelmäßige Aktualisierung zu gewährleisten. Verschiedene Unternehmen bieten hierzu Dienstleistungen und Produkte an, die zum Teil auch die entsprechenden US-amerikanischen Listen abdecken.

Hinsichtlich des Umfangs eines Embargos unterscheidet man zwischen

- **Totalembargos** (derzeit keine, z. B. bis 2003 gegen den Irak)
- **Teilembargos** (für bestimmte Waren oder bestimmte Personen, z. B. Ausfuhr bestimmter Luxusgüter nach Nordkorea)
- **Waffenembargos** (derzeit z. B. Sudan, Irak, Somalia)
- **Erfüllungsverboten** (verbieten Erfüllung von Schadensersatzansprüchen infolge eines Embargos bzw. schützen vor solchen Ansprüchen, derzeit z. B. Libyen)

Rechtsfolge eines Embargos ist grundsätzlich ein generelles **Ausfuhrverbot** für die betroffenen Produkte. Es können jedoch z. B. auch besondere Genehmigungspflichten begründet werden.

1.2.1 Listengebundene Beschränkungen

Es existieren umfangreiche Listen, in denen eine Vielzahl von Gütern aufgeführt wird, die außenwirtschaftsrechtlichen Beschränkungen unterliegen. Von besonderer Bedeutung für die Wirtschaft ist dabei die in **Anhang I der EG Dual-use-VO** enthaltene Liste von **Dual-use-Gütern**, d.h. solchen Gütern, die sowohl zivil als auch militärisch nutzbar sind. In Deutschland existiert ferner die **Ausfuhrliste (AL),** die in ihrem Teil A Rüstungsgüter und in ihrem Teil C die in der EG Dual-use-VO genannten Dual-use-Güter sowie einige zusätzliche nationale Positionen (900er Kennungen) aufzählt.

Praxishinweis

> Auch wenn die AL den Anhang I der EG Dual-use-VO grundsätzlich mit umfasst, darf sich ein Exporteur nicht ausschließlich auf die AL verlassen. So sind etwa Änderungen zeitlich nicht aufeinander abgestimmt und erfolgen in der AL mit einer gewissen Verzögerung. Beide Listen stellen in Deutschland geltendes Recht dar und müssen daher beachtet werden.

Weitere Listen sind beispielsweise im Chemiewaffenübereinkommen (CWÜ) oder im Kriegswaffengesetz (KrWaffG) enthalten.

Rechtsfolge der Nennung in einer Liste ist häufig eine **Genehmigungspflicht**, z. B. gemäß Art. 3 Abs. 1 EG Dual-use-VO oder § 5 AWV.

1.2.2 Verwendungsbezogene Beschränkungen

Und schließlich können Beschränkungen auch für nicht gelistete Güter bestehen, nämlich dann, wenn der Ausführer entweder **vom BAFA** davon **unterrichtet** wurde oder **positive Kenntnis** davon hat, dass die Güter für bestimmte geächtete Verwendungszwecke bestimmt sind. Zu diesen Verwendungszwecken gehören:

Nach **Art. 4 EG Dual-use-VO**

- die Verwendung bei der Herstellung von **Massenvernichtungswaffen** oder **Trägersystemen** für solche Waffen sowie
- die **militärische** Verwendung in einem Staat, gegen den ein **Waffenembargo** besteht.

Nach §§ 5c, 5d **AWV**

- die **militärische** Verwendung in einem Land der deutschen **Länderliste K** (Liste besonders kritischer Länder, derzeit Kuba, Syrien) sowie
- die Verwendung in einer **kerntechnischen Anlage** in Algerien, Indien, Irak, Iran, Israel, Jordanien, Libyen, Nordkorea, Pakistan oder Syrien.
- Anders als im europäischen Recht existiert bei Genehmigungspflichten nach der AWV eine **Bagatellklausel** für Lieferungen, deren Wert unter EUR 2.500 liegt. Ausnahmen sind Software und Technologie.

Positive Kenntnis von einem der oben genannten Verwendungszwecke liegt bei grober Fahrlässigkeit zwar grundsätzlich nicht vor und der Ausführer ist auch nicht zu Nachforschungen verpflichtet. Der Exporteur darf die Augen jedoch auch nicht bewusst vor eindeutigen Hinweisen verschließen.[7]

Rechtsfolge bei einer Unterrichtung des BAFA von einer möglichen geächteten Verwendung ist eine **Genehmigungspflicht**. Bei positiver Kenntnis des Ausführers von einer geplanten Verwendung zu einem der oben genannten Zwecke besteht eine Verpflichtung zur **Unterrichtung** des BAFA, das über das Bestehen einer Genehmigungspflicht entscheidet.

---

[7] Zum Begriff der Kenntnis vgl. z. B. *Weith / Wegner / Ehrlich*, Grundzüge der Exportkontrolle, 2006, Ziffer. D. 74.

1.3 Verbringungen

Unter einer Verbringung versteht man im Gegensatz zur Ausfuhr den Export in einen anderen Mitgliedstaat der EU. Für diesen Fall stellt das Exportkontrollrecht deutlich geringere Anforderungen:

Generelle listengebundene Genehmigungspflichten bestehen nur in zwei Fällen, nämlich

- gemäß **§ 7 Abs. 1 AWV** für Rüstungsgüter im Sinne des Teil A der AL sowie
- gemäß **Art. 21 EG Dual-use-VO** für besonders sensitive, in Anhang IV der Verordnung gelistete Dual-use-Güter.

Im Übrigen kommen Beschränkungen nur dann in Betracht, wenn das **endgültige Bestimmungsziel** der Güter **außerhalb der Europäischen Union** liegt. In diesem Fall bestehen

- gemäß **§ 7 Abs. 2 AWV** eine Genehmigungspflicht für in der AL genannte Dual-use-Güter und
- gemäß **§ 7 Abs. 3 und Abs. 4 AWV** verwendungsbezogene Beschränkungen, die denen der Regelungen für die Ausfuhr in §§ 5c und 5d AWV nachgebildet sind, also für die Verwendung in kerntechnischen Anlagen in bestimmten Staaten sowie für die militärische Verwendung in einem Land der Länderliste K.

Beispiel:

Unternehmen A stellt bestimmte Werkzeugmaschinen (gelistet in Anhang I der EG Dual-use-VO) und einzelne Baugruppen für solche Maschinen (nicht gelistet) her. A hat folgende Bestellungen erhalten:

a) Lieferung einer Werkzeugmaschine an ein international renommiertes norwegisches Unternehmen

b) Lieferung einer Baugruppe an die iranische Fajr Industrial Group, angegebener Verwendungszweck: Einsatz bei der Produktion von Kühlgeräten

c) Lieferung einer Baugruppe an die Firma Al'Halal aus Syrien, die Handfeuerwaffen für die syrischen Streitkräfte fertigt

Gegen keinen der Empfänger besteht ein personenbezogenes Embargo. Sind exportkontrollrechtliche Restriktionen / Pflichten zu beachten?

AUSZUG AUS DEM IRAN-EMBARGO DER EU:

„Artikel 7

[…]

(3) Den in den Anhängen IV und V aufgeführten natürlichen und juristischen Personen, Organisationen und Einrichtungen dürfen weder unmittelbar noch mittelbar Gelder oder wirtschaftliche Ressourcen zur Verfügung gestellt werden oder zugute kommen.

[…]

ANHANG IV

A. Juristische Personen, Organisationen und Einrichtungen

[…]

3. Fajr Industrial Group. Sonstige Informationen: a) früher: Instrumentation Factory Plant, b) der OLI unterstehende Einrichtung, c) am Programm Irans für ballistische Raketen beteiligt

Lösung:

In allen drei Fällen liegen Ausfuhren vor, da das Bestimmungsland kein Mitgliedstaat der EU ist.

a) Für Norwegen und den Empfänger sind keine Embargovorschriften zu beachten. Die Maschine ist jedoch in Anhang I der EG Dual-use-VO gelistet, so dass gemäß Art. 3 Abs. 1 EG Dual-use-VO eine Genehmigung erforderlich ist. A kann allerdings als Verfahrensvereinfachung die Allgemeine Genehmigung EU001 in Anspruch nehmen (dazu unten ausführlicher).

b) Gegen den Empfänger besteht ein Embargo der EU, so dass keinerlei Geschäfte getätigt werden dürfen. Dass die Güter nicht gelistet sind und ein harmloser Verwendungszweck genannt wurde, ist in diesem Fall irrelevant.

c) Gegen Syrien besteht in Europa kein Embargo, die Firma Al'Halal wird ferner nicht auf den sog. Terrorlisten genannt. Auch listengebundene Beschränkungen bestehen für die Baugruppen nicht. Es ist aber von einer militärischen Verwendung der Güter auszugehen, da diese aller Voraussicht nach in Maschinen zur Waffenproduktion zum Einsatz kommen werden. Da Syrien auf der deutschen Länderliste K genannt ist, besteht eine Pflicht zur Unterrichtung des BAFA gemäß § 5c Abs. 2 AWV, sofern nicht die Bagatellklausel einschlägig ist (Wert nicht mehr als EUR 2.500).

1.4 Dienstleistungen

Nicht nur die Ausfuhr von technischen Unterlagen kann zur Verbreitung militärisch nutzbarer Technologien beitragen, sondern auch Dienstleistungen, d.h. die **mündliche Weitergabe von technischem Know-how** oder die **Anwendung dieses Wissens in Drittstaaten**. Aus diesem Grund besteht Einigkeit darüber, dass auch die so genannte „**Technische Unterstützung**" durch das Außenwirtschaftsrecht kontrolliert werden muss.

Nach einem EuGH-Gutachten aus dem Jahre 1994 verfügt die Europäische Union allerdings nicht über die Kompetenz zur Regelung des Dienstleistungsverkehrs außerhalb Europas.[8] Daher haben die einzelnen Mitgliedstaaten auf Grundlage einer Gemeinsamen Aktion des Rates[9] diesbezüglich harmonisierte nationale Vorschriften erlassen. In Deutschland sind dies die **§§ 45 bis 45e AWV**.

Auf eine Darstellung der Regelungen im Detail wird hier verzichtet.[10] Der Anwendungsbereich der Normen ist jedoch relativ begrenzt, weil sie weitgehend die kumulative Erfüllung der listen- und der verwendungsbezogenen Beschränkungen bei der Ausfuhr voraussetzen und damit **nur besonders sensitive Technologien, Staaten und Verwendungszwecke** betreffen. Zudem gibt es diverse **Ausnahmen**, unter anderem für

- die Weitergabe von **allgemein zugänglichen Informationen**, also solchen, die z. B. bereits in Büchern, Fachzeitschriften, Internet veröffentlicht sind
- Informationen, die lediglich der **Grundlagenforschung** dienen, also nicht primär auf eine praktische Anwendung gerichtet sind
- technische Unterstützung für die **Bundeswehr im Auslandseinsatz**
- Unterstützung bei der **erstmaligen Herstellung der Betriebsbereitschaft** von genehmigt ausgeführten Gütern

Als Besonderheit ist zu beachten, dass eine außenwirtschaftsrechtlich relevante und gegebenenfalls genehmigungspflichtige technische Unterstützung auch im **Inland** erbracht werden kann, wenn Personen aus bestimmten Staaten dadurch an sensibles technisches Know-how gelangen können, etwa bei Forschungsprojekten an einer deutschen Universität unter Beteiligung ausländischer Doktoranden.

Die **Rechtsfolgen** entsprechen denen der §§ 5c und 5d AWV: Bei einer Unterrichtung des Ausführers vom Vorliegen der verwendungsbezogenen Voraussetzungen durch das BAFA besteht eine **Genehmigungspflicht**. Bei positiver Kenntnis des Ausführers vom Vorliegen der Voraussetzungen besteht eine Verpflichtung zur **Unterrichtung** des BAFA, das über das Bestehen einer Genehmigungspflicht entscheidet.

---

[8] Gutachten 1/94 (WTO), Slg. 1994 I-5267, Rn. 44 ff.

[9] Gemeinsame Aktion 2000/401/GASP des Rates vom 22. Juni 2000 betr. die Kontrolle von technischer Unterstützung in Bezug auf bestimmte militärische Endverwendungen.

[10] Ausführliche Darstellung z. B. bei *Weith / Wegner / Ehrlich*, a.a.O., Ziffer D. 100 ff.

1.5 Brokering

Ferner enthalten die **§§ 40 bis 42 AWV** Vorschriften zu den so genannten **Handels- und Vermittlungsgeschäften**. Darunter versteht das Gesetz nicht nur den Abschluss, sondern auch die bloße Vermittlung von Geschäften oder den Nachweis einer Gelegenheit zum Abschluss eines Geschäfts.[11]

Eine Genehmigungspflicht besteht bei solchen Geschäften in folgenden Konstellationen:

- Gemäß **§ 40 AWV**: für Handels- und Vermittlungsgeschäfte über **Rüstungsgüter** (Abschnitt A der AL), die sich in einem **Drittland**, d.h. außerhalb der EU befinden.
- Gemäß **§ 41 AWV**: für Handels- und Vermittlungsgeschäfte über in Anhang IV der EG Dual-use-VO gelistete **besonders sensible Dual-use-Güter**, die sich in einem **Drittland** befinden.
- Gemäß **§ 42 AWV**: für Handels- und Vermittlungsgeschäfte von gebiets-ansässigen Deutschen **in einem Drittland**, sofern sie sich auf bestimmte **Kriegswaffen** beziehen und Käufer- oder Bestimmungsland ein **Embargostaat** oder ein **Land der Länderliste K** ist.

Beispiel:

Mitarbeiter M von der deutschen Werft W muss dringend zu einer Besprechung, als er einen Anruf aus dem Verteidigungsministerium des asiatischen Landes A erhält, an das man vor mehreren Jahren eine Fregatte geliefert hat. Der Anrufer möchte 500 kg grauen Spezialtarnlack (gelistet als Rüstungsgut in Teil A der AL) bestellen. M möchte das Gespräch schnell beenden und erklärt, man habe diese Farbe selbst nicht vorrätig und beziehe sie von dem Unternehmen S in der Schweiz. Der übliche Preis betrage EUR 80,- pro kg, der Anrufer möge sich an den dortigen Vertriebsleiter V wenden. (Beispiel nach Weith / Wegner / Ehrlich)

Lösung:

Die Schweiz ist nicht Mitglied der EU und damit ein Drittland. Die Aussagen des M dürften als Nachweis einer Gelegenheit zum Abschluss eines Geschäfts über ein Rüstungsgut zu werten sein. M hat folglich mit diesem kurzen Telefonat ohne erforderliche Genehmigung ein Handels- und Vermittlungsgeschäft vorgenommen. Dies kann gemäß § 33 Abs. 1 AWG als Ordnungswidrigkeit mit einer Geldbuße von bis zu EUR 500.000,00 geahndet werden. Gegebenenfalls ist sogar eine Ahndung als Straftat nach § 34 Abs. 2 AWG möglich.

---

11 Vgl. die Definition in § 4c Nr. 6 AWV.

1.6 US-Reexportrecht

Im Exportkontrollrecht gilt grundsätzlich das Territorialitäts- und Nationalitätsprinzip, d.h. dass beispielsweise das deutsche AWG und die AWV nur auf Handlungen in Deutschland und ausnahmsweise auf deutsche Staatsbürger im Ausland Anwendung finden. Anders ist dies jedoch im US-amerikanischen Exportkontrollrecht. Dieses hat nach seiner Konzeption mittelbar auch extraterritoriale Wirkung auf Nicht-US-Bürger, indem es an bestimmte Waren mit einem Bezug zu den USA anknüpft.[12]

Den **Export Administration Regulations (EAR)** der USA unterliegen **weltweit** folgende Güter:

- Waren mit Ursprung in den USA
- Produkte mit einem Mindestanteil US-amerikanischer Bestandteile (25 %, bzw. 10 %, wenn die Waren in aus US-Sicht besonders sensible Staaten geliefert werden sollen)
- Mit US-Technologie oder Software hergestellte ausländische Waren (foreign produced direct products)

Will also beispielsweise ein deutsches Unternehmen Waren, die es von einem Hersteller aus den USA bezogen hat, seinerseits in ein anderes Land exportieren, so liegt aus Sicht der USA ein so genannter **Reexport** vor, für den gegebenenfalls eine Genehmigung bei den Exportkontrollbehörden der USA eingeholt werden muss.

Die Einhaltung des US-Reexportrechts wird von den europäischen Behörden nicht geprüft, so dass eine Missachtung keine direkten Auswirkungen auf das konkrete Ausfuhrgeschäft hat. Die Nichtbeachtung des Exportkontrollrechts der USA kann jedoch überaus schwer wiegende Beeinträchtigungen des USA-Geschäfts von international tätigen Unternehmen nach sich ziehen. Zu den möglichen **Rechtsfolgen** gehören unter anderem:

- **Eintrag auf der Denied Persons List** (DPL, so genannte „Schwarze Liste“), die ein Verbot für US-Unternehmen bedeutet, mit dem gelisteten Unternehmen weiterhin Geschäfte jeglicher Art abzuschließen
- **Einfrieren von Vermögen** in den USA
- **Strafrechtliche Sanktionen** gegen die Geschäftsführung, die vollstreckt werden, sobald ein Geschäftsführer amerikanischen Boden betritt

---

12 Grundlegend zum US-Exportkontrollrecht Bundesamt für Wirtschaft und Ausfuhrkontrolle (Hrsg.), HADDEX (FN 5), Teil 12.

2. Genehmigungsverfahren

2.1 Ablauf des Verfahrens

Ist nach den vorstehenden Ausführungen für ein Exportgeschäft eine Genehmigung erforderlich, so muss diese grundsätzlich beim BAFA in Eschborn als zuständiger Behörde beantragt werden. Die **Dauer** eines Genehmigungsverfahrens beträgt je nach Umfang der Lieferung und Sensibilität der Güter und des Bestimmungslandes zwischen 14 Tagen und mehreren Monaten.

Der Antrag auf Erteilung einer Genehmigung ist dabei stets vom **Ausführer** im exportkontrollrechtlichen Sinne zu stellen. Dieser ist nicht zwingend identisch mit dem zollrechtlichen Ausführer im Sinne von Art. 788 der Zollkodex-Durchführungsverordnung. Es kommt für das Exportkontrollrecht nicht entscheidend darauf an, wer zivilrechtlicher Eigentümer der auszuführenden Güter ist, sondern **wer über das „ob“ und „wie“ der Versendung der Waren entscheidend bestimmt**. In der Regel ist dies der Vertragspartner des Empfängers der Güter im Bestimmungsland.[13]

2.2 Arten von Genehmigungen

Bei Genehmigungen des BAFA kann grundsätzlich zwischen individuell beantragten Genehmigungen und Allgemeinen Genehmigungen unterschieden werden.

Individuell beantragte Genehmigungen können in drei verschiedenen Formen erteilt werden:

- Grundform ist die **Einzelgenehmigung** für einen konkreten Exportvorgang.
- Eine Sonderform ist die **Höchstbetragsgenehmigung**, die mehrfache oder gestückelte Lieferungen an denselben Empfänger bis zu einer bestimmten Gesamtmenge gestattet.

> **Beispiel:**
>
> Es wird ein Vertrag über die Lieferung von insgesamt 500 t einer bestimmten Chemikalie geschlossen, die der Empfänger über den Zeitraum von drei Jahren in beliebig großen Tranchen abrufen darf.

---

13 *Tervooren / Mrozek*, a.a.O., Art. 2 Dual-use-VO Rn. 31 ff.

- Und schließlich besteht die Möglichkeit, eine **Sammelausfuhrgenehmigung** zu beantragen, die auf einen bestimmten Zeitraum befristet für verschiedene Produkte eine unbestimmte Zahl von Ausfuhren an verschiedene Empfänger gestattet. Wegen ihres weiten Gestattungsbereiches werden hohe Anforderungen an die Zuverlässigkeit des Ausführers gestellt.

Beispiel:

Typischer Anwendungsbereich für Sammelausfuhrgenehmigungen sind internationale Rüstungskooperationen, bei denen einzelne Komponenten in unterschiedlichen Staaten gefertigt werden.

Allgemeine Genehmigungen für bestimmte Güter werden dagegen vom BAFA veröffentlicht. Ein wichtiges Beispiel ist die Allgemeine Ausfuhrgenehmigung Nr. EU001, die in weitem Umfang Ausfuhren in folgende Staaten erlaubt: Norwegen, Schweiz, USA, Kanada, Japan, Australien, Neuseeland. Auf diese Allgemeine Genehmigung kann sich grundsätzlich jeder Ausführer berufen und muss keine gesonderte Genehmigung beantragen. Er muss allerdings die Inanspruchnahme der Allgemeingenehmigung beim BAFA einmalig anzeigen und die ausgeführten Güter halbjährlich melden.[14]

3. Risiken und Compliance

3.1 Drohende Sanktionen

Bei Verstößen gegen das Außenwirtschaftsrecht drohen empfindliche Sanktionen. Insbesondere kennt § 34 AWG folgende **Straftatbestände** und Strafandrohungen:

- **Illegale Ausfuhr oder Verbringung**: Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe
- **Förderung** einer fremden Tat, z. B. durch Zulieferung der auszuführenden Waren: Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe
- **Embargobruch**: Freiheitsstrafe von sechs Monaten bis zu fünf Jahren

14 Bundesamt für Wirtschaft und Ausfuhrkontrolle (Hrsg.), HADDEX (FN 5), Rn. 465 g bis 465 i.

- **„Schwerer Fall“ der illegalen Ausfuhr oder des Embargobruchs**: Freiheitsstrafe nicht unter zwei Jahren, d.h. regelmäßig keine Strafaussetzung zur Bewährung möglich: Das Gesetz nennt hier als Beispiel ausdrücklich auch den Fall des **gewerbsmäßigen Handelns**. Folglich ist die Gefahr für einen Unternehmer vergleichsweise groß, dass im Falle einer strafrechtlichen Verurteilung nicht nur eine Geldstrafe verhängt wird.
- **Fahrlässige Begehung**: Freiheitsstrafe bis zu drei Jahren oder Geldstrafe

Außerhalb des strafrechtlichen Bereichs drohen zudem folgende Sanktionen:

- **Bußgelder** bis zu EUR 500.000,00 oder sogar bis zu EUR 1.000.000,00 bei strafbarem Handeln von Mitarbeitern infolge unzureichender Beaufsichtigung
- **Verfallserklärung**, d.h. Abschöpfung des Bruttoerlöses des Geschäfts

Bei Verstößen gegen das US-Reexportrecht drohen zudem Sanktionen in den USA. Dies können sein:

- **civil penalties**
- **criminal penalties** (langjährige Haftstrafen möglich)
- **Denial Order** (befristetes Verbot von Exportgeschäften)
- **Aufnahme in die Denied Persons List**, d.h. Ausschluss von jeglichem USA-Geschäft, häufig auch für sehr lange Zeiträume von bis zu 20 Jahren

Nicht unterschätzt werden sollte schließlich auch der **Imageschaden**, den die Berichterstattung über einen „Exportskandal“ in den Medien verursachen kann.

3.2 Risikomanagement / Compliance

Um die oben dargestellten Sanktionen zu vermeiden und Compliance im Bereich des Außenwirtschaftsrechts zu erreichen, ist die Implementierung einer **innerbetrieblichen Exportkontrolle** in allen exportierenden Betrieben zwingend erforderlich. Aber auch bei Bestehen von solchen Kontrollsystemen ist nie völlig auszuschließen, dass ein exportiertes Produkt letztlich – und sei es über Umwege – in falsche Hände gerät. Dann allerdings ist es wichtig, auf diese Situation vorbereitet zu sein und gegenüber den Behörden und den Medien darlegen zu können, dass von Unternehmensseite **alles Denkbare** getan wurde, um einen solchen Missbrauch zu vermeiden. Aus diesem Grund sollte auch frühzeitig der **Kontakt zur zuständigen Behörde** hergestellt und Zweifelsfragen offen kommuniziert werden. Das BAFA bewertet solche Nachfragen oder zur Absicherung gestellte Ausfuhranträge regelmäßig nicht als Zeichen mangelnder Kompetenz, sondern vielmehr positiv als Zeichen dafür, dass ein Unternehmen umfassend um Compliance bemüht ist.[15]

---

15 Bundesamt für Wirtschaft und Ausfuhrkontrolle (Hrsg.), Praxis der Exportkontrolle, 2006, S. 46.

Erster Schritt ist stets die Benennung eines **Ausfuhrverantwortlichen** aus den Reihen der Unternehmensleitung gegenüber dem BAFA.[16] Dies ist auch Voraussetzung für die Erteilung von Genehmigungen. Dem Ausfuhrverantwortlichen obliegen im Wesentlichen **vier Hauptpflichten**:

- **Personalauswahlpflicht**:
  Der Ausfuhrverantwortliche muss dafür sorgen, dass im exportsensiblen Bereich hinreichend fachkundiges und zuverlässiges Personal beschäftigt ist.

- **Organisationspflicht**:
  Der Ausfuhrverantwortliche muss zum einen die Exportkontrolle im Organigramm des Unternehmens richtig anordnen (**Aufbauorganisation**) und zum anderen durch geeignete Mittel die Arbeitsabläufe so organisieren, dass Verstöße gegen das Außenwirtschaftsrecht ausgeschlossen sind (**Ablauforganisation**).

- **Überwachungspflicht**:
  Der Ausfuhrverantwortliche muss durch geeignete Maßnahmen kontrollieren, ob die organisatorischen Anordnungen tatsächlich eingehalten werden (z. B. Stichproben, regelmäßige Systemprüfungen und Routineprüfungen, Dokumentation).

- **Weiterbildungspflicht**:
  Der Ausfuhrverantwortliche muss für die eigene Weiterbildung und die seiner Mitarbeiter auf dem Gebiet des Außenwirtschaftsrechts sorgen. Hierzu gehört auch, dass die außenwirtschaftsrechtlichen Vorschriften im Betrieb vorhanden sind und ständig aktualisiert werden.

4. Fazit

Die vorstehenden Ausführungen sollen für die Themen Exportkontrolle und Compliance sensibilisieren. Sie können jedoch keine vollständige Darstellung des Außenwirtschaftsrechts oder der vielfältigen Maßnahmen bieten, die zur Compliance in diesem wichtigen Geschäftsbereich in einem Unternehmen getroffen werden können. Es ist vielmehr für die Geschäftsleitung jedes Unternehmens unverzichtbar, sich vertieft mit dem Thema Exportkontrolle auseinanderzusetzen und ein Risikomanagementsystem zu entwickeln, das speziell auf die Bedürfnisse des jeweiligen Unternehmens zugeschnitten ist.

---

[16] Ausführlich zur Bedeutung des Ausfuhrverantwortlichen und seinen Aufgaben vgl. Bundesamt für Wirtschaft und Ausfuhrkontrolle (Hrsg.), HADDEX (FN 5), Rn. 71, 345 ff.

Compliance – Auslandsrisiken erkennen und steuern (Schwerpunkt Asien)

Thomas Weidlich / Angelika Yates

Zusammenfassung

Compliance ist ein Thema, mit dem sich Unternehmen nicht nur in ihren Heimatländern, sondern in jedem Land, in dem sie geschäftlich aktiv sind, befassen müssen. Compliance-Anforderungen bestehen in verschiedenen Ländern bereits beim Eintritt in den ausländischen Markt und erstrecken sich auf komplexe Themen wie unter anderem die vertragliche Gestaltung von Rechtsverhältnissen, der Beschäftigung von Mitarbeitern im Ausland und die Durchsetzung von Ansprüchen vor Ort. Die Nichtbeachtung lokaler Anforderungen kann zu gravierenden Nachteilen führen und den Erfolg einer Investition im Ausland gefährden.

1. Compliance im Zeitalter der Globalisierung

Deutschland ist Exportweltmeister und sowohl große Konzerne als auch mittelständische Unternehmen operieren heute in der ganzen Welt. Mit Ausdehnung der Geschäftsaktivitäten ins Ausland stellt sich immer wieder die Frage nach den dort zu beachtenden Compliance-Anforderungen.[1] Während die Risiken bei einer Nichtbeachtung von Compliance-Regeln im innereuropäischen Ausland häufig mit deutschem Recht vergleichbar sein mögen, kann der rechtliche Rahmen in Ländern außerhalb Europas erheblich von der deutschen Situation abweichen und Verstöße dagegen gravierende Folgen haben. Auch Großkonzerne machen immer wieder unliebsame Erfahrungen, zuletzt etwa der Frankfurter Flughafenbetreiber Fraport auf den Philippinen (dazu noch näher unten im Text).

---

1 Zur Errichtung einer Compliance-Organisation *Hauschka*, ZIP 2004, 877 ff.

Vor dem Hintergrund der vielfältigen Compliance-Risiken bei Geschäftstätigkeiten im Ausland ist die frühzeitige und intensive Auseinandersetzung mit den in den einzelnen Ländern geltenden Bestimmungen und Anforderungen notwendig, um Haftungsrisiken für das Unternehmen zu vermeiden und den Erfolg einer Investition im Ausland nicht zu gefährden. Mit zunehmender Internationalität nimmt die Komplexität innerhalb einer Unternehmensgruppe zu. Knappe Managementkapazitäten, fehlende Transparenz und divergierende nationale Regelungen sind typische Merkmale, die sich im Zuge der Globalisierung verstärken – bei gleichzeitiger Zunahme der Risiken.

2. Regulatorische Minenfelder beim Markteintritt im Ausland

Viele asiatische Märkte wie beispielsweise die beiden Boomländer China und Indien sind ausländischen Investoren nicht frei zugänglich. So unterliegen Ausländer in bestimmten Industriebereichen oftmals Beteiligungsobergrenzen oder sind von sensiblen Wirtschaftsbereichen sogar gänzlich ausgeschlossen. Der Umgang mit solchen Beschränkungen ist nicht immer einfach.

Für eine Geschäftstätigkeit in **China** sind eine Vielzahl von Genehmigungen und Registrierungen erforderlich, die vor Beginn und auch für den täglichen Geschäftsablauf zu beantragen sind. Bereits die Gründung von Unternehmen durch ausländische Investoren ist in China – anders als in Deutschland – nur nach entsprechender Genehmigung durch die zuständige Handelsbehörde und Registrierung durch die Gewerbebehörden möglich. Daraufhin muss dann eine Geschäftslizenz (Business Licence) beantragt werden, ohne die eine Gesellschaft in China nicht agieren darf. Ob und in welcher Form die Genehmigung erteilt wird, hängt von dem konkret geplanten Vorhaben ab. Generell unterliegen ausländische Investitionen in China einer umfassenden Reglementierung.[2] Die maßgeblichen Vorschriften zur Investitionslenkung, die so genannten *Provisions on Directing Foreign Investment* werden durch einen Lenkungskatalog, den *Catalogue for Directing Foreign Investment* ergänzt. Letzterer enthält eine Liste aller Industriesektoren und teilt diese in die Kategorien *prohibited* (verboten), *restricted* (beschränkt) und *encouraged* (gefördert) ein. Investitionsvorhaben, die in keine dieser Kategorien fallen, sind grundsätzlich zulässig und gehören damit der Kategorie *permitted* (erlaubt) an. Änderungen des Investitionskataloges wurden zuletzt im November 2007 beschlossen. Während der Finanzdienstleistungssektor weiter liberalisiert wurde, unterstreicht die Herabstufung von energieintensiven und ressourcenaufwändigen Industriebereichen von der ehemals geförderten in die beschränkte oder sogar verbotene Kategorie, dass der Umweltschutz auch in China eine immer wichtigere Rolle spielt.[3]

---

2 Hierzu *Dickinson/Vietz*, GmbHR 2006, 245, 248 f.

3 *Menshause*, China im Umgang mit Auslandsinvestitionen wählerisch, http://www.bfai.de.

Zu den derzeit für ausländische Investoren generell verbotenen Betätigungsfeldern gehören unter anderem der Bau und Betrieb von Stromnetzen, die Luftverkehrsüberwachung, der Betrieb von Postunternehmen sowie von Fernseh- und Radiostationen und das Druck- und Verlagswesen. Beschränkt zulässig sind dagegen beispielsweise die Konstruktion und der Betrieb von Raffinerien und die Betätigung in bestimmten Sektoren der chemischen und pharmazeutischen Industrie. In die Kategorie der geförderten Investitionsvorhaben fallen derzeit unter anderem die Förderung von Erdöl und Naturgas, die Herstellung von Kunststoffen für den industriellen Gebrauch und die Entwicklung und Produktion von Pestiziden und anderen chemischen Stoffen für die Landwirtschaft. Von der Einteilung in diese Kategorien hängt ab, ob und inwieweit das Projekt staatlichen Regulierungen unterliegt oder durch Vergünstigungen gefördert wird. Regulierungen können unter anderem hinsichtlich der zulässigen Beteiligungsform oder der maximalen Beteiligungshöhe eines ausländischen Investors bestehen, während geförderte Projekte unter Umständen steuerlich bevorzugt behandelt werden oder andere Vorteile erfahren.

Indiens Wirtschaftspolitik zielt im Grundsatz auf eine Förderung ausländischer Direktinvestitionen und begrüßt diese heute in nahezu allen Wirtschaftszweigen. Ausgenommen sind allerdings einige Bereiche, die politisch oder wirtschaftlich von wesentlicher strategischer Bedeutung sind. Zu dieser *Prohibited List* zählt etwa der Atomsektor,[4] die Verteidigungsindustrie, der Schienenverkehr, Lotterie und Glücksspiele, zum Teil auch Geschäfte mit Immobilien und, bis auf einige Ausnahmen, der Landwirtschaftssektor. In diesen Bereichen ist eine ausländische Direktinvestition generell nicht zulässig. In vielen Wirtschaftszweigen und für fast alle Produktionsvorhaben sind ausländische Direktinvestitionen ohne Genehmigung durch die Behörden zulässig (so genannte *Automatic Route*). Ausnahmen zu der *Automatic Route* sind gesetzlich festgelegt und unterliegen der so genannten *Approval Route*. Diese Ausnahmen erfordern eine Genehmigung durch das *Foreign Investment Promotion Board* (FIPB). In bestimmten Wirtschaftszweigen bedürfen ausländische Beteiligungen an indischen Unternehmen bei Überschreitung bestimmter Beteiligungsquoten (so genannte *Sectoral Caps*) ebenfalls einer besonderen Genehmigung. So können z. B. 100%ige Beteiligungen oder der Erwerb einer Mehrheitsbeteiligung im Finanz-, Versicherungs- und Telekommunikationssektor alleine aus diesem Grund genehmigungspflichtig sein. Im Einzelhandel sind inzwischen Joint Ventures für den Verkauf einzelner Markenprodukte (*single brand retail*) möglich, an denen Ausländer bis zu 51% der Gesellschaftsanteile halten können. Ob in Indien eine besondere Genehmigung eingeholt werden muss, richtet sich also vor allem nach dem Wirtschaftszweig, in welchem das auslandsinvestierte Unternehmen tätig werden soll, und nach der angestrebten Beteiligungshöhe.[5]

Die indische Regierung schützt den indischen Partner eines Joint Ventures zudem davor, dass der ausländische Investor weitere Kooperationen im gleichen Geschäftsfeld eingeht. Mit einigen Ausnahmen benötigen ausländische Investoren für Folgeinvestitionen ebenfalls eine

---

4 *Adam*, Energiepoker: Das beste Blatt gewinnt, ASIA BRIDGE 9/2007, S. 8.

5 OAV Wirtschaftshandbuch Asien- Pazifik 2006/2007, S.189.

staatliche Erlaubnis, die in der Praxis nicht ohne die Zustimmung des indischen Partners erteilt wird.[6] Dieser Umstand sollte bereits bei Begründung des ersten Joint Ventures in Indien berücksichtigt werden.

Auch in **Indonesien** existieren umfangreiche Beschränkungen für Ausländer. Das erst vor kurzem revidierte *Investment Law*[7] ermächtigt die Regierung, eine neue *Negative List* aufzustellen. Bei der *Negative List* handelt es sich um eine Aufzählung von für ausländische Unternehmen verbotenen bzw. beschränkten Tätigkeiten, um die indonesischen Marktteilnehmer zu schützen. Teilweise beinhaltet die *Negative List* komplette Verbote; andere Wirtschaftsbereiche sind nur für kleine und mittelständische Unternehmen zugänglich und wieder andere Geschäftzweige können nur zusammen mit indonesischen Teilhabern ausgeübt werden. Im Unterschied zur bisherigen *Negative List* mit 83 Bereichen erfolgt eine Aufteilung der Wirtschaftsbereiche durch die neue *Negative List* in 338 Sektoren. Hiermit soll mehr Transparenz in die für Investoren gesperrten Bereiche gebracht werden.[8] Die aufgeführten Beschränkungen gelten seit dem 3. Juli 2007 für die Gründung neuer Gesellschaften sowie für Investitionen in bereits bestehende Unternehmen. Eine Rückwirkung entfaltet die neue *Negative List* jedoch nicht, so dass bereits vor Inkrafttreten der neuen Liste genehmigte Investitionen, Gesellschafterverhältnisse etc. nicht angepasst werden müssen. Sofern die *Negative List* für bestimmte Geschäftszweige keine höhere indonesische Beteiligung vorschreibt, gilt im Übrigen die Regelung, wonach Gesellschaften mit 100% ausländischer Beteiligung innerhalb eines Zeitraumes von 15 Jahren mindestens 5% der Anteile an indonesische Gesellschafter übertragen müssen.

Die politisch instabile Rechtslage in **Thailand** hat ausländische Investoren zuletzt eher verunsichert als zu weiteren Investitionen ermutigt.[9] Nach dem Regierungswechsel überraschte das Militärregime im Dezember 2006 mit der Einführung eines neuen Investitionsgesetzes,[10] um gegen spekulative Kapitalzuflüsse vorzugehen. Der Entwurf sah vor, dass ausländische Investoren 30 % der Investitionssumme bei der Bank of Thailand hinterlegen müssen und den Betrag ohne Strafzahlung erst nach einem Jahr wieder abziehen dürfen. Die verärgerten Anleger zogen sich zurück und lösten so den schwersten Aktieneinbruch in der Geschichte der thailändischen Börse aus, woraufhin sich das Regime gezwungen sah, die Regelungen bereits nach einem Tag wieder zurückzuziehen. Kurze Zeit später beschloss das Kabinett dann Änderungen zum *Foreign Business Act* (FBA), dem wichtigsten Gesetz zur Regelung ausländischer Geschäftsaktivitäten in Thailand. Auch schon bisher waren zahlreiche Betätigungen für ausländische Investoren (in der Terminologie des FBA so genannte *Aliens*) verboten beziehungsweise nur mit besonderer Genehmigung erlaubt.[11] Zu den verbotenen Geschäftsfeldern

---

6 Press Note 1 (2005) Series vom 12. Januar 2005.

7 *Sauernost*, Heiß ersehnt: Das neue Investitionsgesetz, ASIA BRIDGE 5/2007, S. 30.

8 *Haase*, Investitionen erleichtert- Neues Gesetz soll strukturelle Defizite beseitigen, ASIA BRIDGE, 5/2007, S. 26.

9 *Adam*, Die Marschrichtung bleibt unklar, ASIA BRIDGE 10/2007, S. 8.; *Adam*, Verlorene Vorbildfunktion, ASIA BRIDGE 11/2006, S. 8.

10 *Haase*, Viel Lärm um nichts: Für Investoren ändert sich nicht viel, ASIA BRIDGE, 3/2007, S. 16.

11 *Lehmann*, Geschäfte in Thailand: Rechtliche Rahmenbedingungen einer Investition, aktuell ASIA, 11/2005, S. 54.

gehören unter anderem Medien und Landwirtschaft. Eine Ministererlaubnis ist beispielsweise erforderlich bei Geschäftsaktivitäten auf den Gebieten der nationalen Sicherheit, Kunst und Kultur sowie hinsichtlich bestimmter natürlicher Ressourcen. Eine weitere Liste enthält Geschäftsgebiete, in denen Ausländer eine so genannte *Foreign Business Licence* benötigen. Diese Liste ist recht umfangreich und schließt u.a. Einzelhandel, Großhandel und den Dienstleistungssektor ein.

Vor Änderung des FBA galt ein Unternehmen nur dann nicht als *Alien*, wenn es in Thailand registriert war und die Mehrheit der Anteile von Thais gehalten wurde. Vor diesem Hintergrund waren ausländische Tochterunternehmen stets sehr daran interessiert, als *Thai companies* eingestuft zu werden. Um die Verbote und Beschränkungen des FBA zu umgehen, hielten häufig thailändische Personen oder Unternehmen die Aktienmehrheit an thailändischen Gesellschaften, während die Stimmenmehrheit und damit die Kontrolle abweichend von der Anteilsverteilung weiterhin beim ausländischen Investor lag. Andere Investoren bedienten sich thailändischer Treuhänder (*Nominees*), die in der Regel durch Vertrag zugesichert hatten, im Sinne des ausländischen Investors zu stimmen. Diesen Umgehungspraktiken wird durch das neue Gesetz nun ein Riegel vorgeschoben. Ein Unternehmen gilt jetzt nur dann nicht als Alien, wenn Thais die effektive Kapital- und Stimmenmehrheit ausüben. Ausgelöst wurde der dieser Änderung zugrundeliegende Kabinettsbeschluss offenbar durch den Einstieg der singapurischen Temasek bei dem bis dahin von Ex-Premier Thaksin kontrollierten thailändischen Telekomkonzern Shin Corp. Temasek wurde unterstellt, ihren thailändischen Partnern das Kapital für den Anteilserwerb zur Verfügung gestellt zu haben, um so die Aktienmehrheit an Shin Corp. zu erlangen.[12] Temasek ist die Staatsholding Singapurs, die für den Stadtstaat weltweite Investitionen in Höhe von ca. EUR 65 Mrd. verwaltet. Der Telekommunikationssektor Thailands ist streng reguliert, der direkte Einstieg eines ausländischen Konzerns bei Shin Corp. wäre nach dem FBA nicht möglich gewesen.

Malaysia kennt vergleichbare Beteiligungsgrenzen für Ausländer und hat in vielen Wirtschaftsbereichen zudem Quoten zugunsten der so genannten *Bumiputras*. Das Wort bedeutet „Söhne der Erde“ und umfasst die einheimischen und ethnischen Malaien, die mit dieser Politik gefördert werden sollen. Ausländische Investoren können daher in vielen Fällen keine 100%ige Beteiligung an einem Unternehmen in Malaysia erwerben, auch wenn Ausnahmen inzwischen einfacher genehmigt werden.[13]

Auch die **Philippinen** kennen Beteiligungsbeschränkungen für Ausländer, die bei einem Investment zu beachten sind. Fraport hat dies als Minderheitsgesellschafterin der philippinischen Gesellschaft PIATCO jüngst auf schmerzhafte Weise erfahren.[14] PIATCO war Inhaberin einer Konzession zum Bau und Betrieb eines neuen Flughafenterminals auf dem Flugha-

---

[12] Straits Times vom 17. November 2006, Police probe Temasek’s Shin Corp buy, http://www.asiamedia.ucla.edu/article-southeastasia.asp?partneid=57868.

[13] Investieren in Malaysia, aktuell ASIA, 05/2006, S. 28.

[14] Handelsblatt vom 28. Juli 2006, Fraport- Mitarbeiter nach Investition in Philippinen angeklagt, http://www.handelsblatt.com/News/Unternehmen/Handel-Dienstleistungen/_pv/grid_id/1227365/_p/200040/_t/ft/_b/1114023/default.aspx/fraport-mitarbeiter-nach-investition-in-philippinen-angeklagt.html.

fen in Manila. Kurz vor Fertigstellung hatten die Philippinen die Konzession sowie sämtliche mit PIATCO geschlossenen Verträge aus verschiedenen Gründen für nichtig erklärt. Fraport hatte daraufhin im September 2003 ein Investitionsschutzverfahren eingeleitet, nachdem Verhandlungen über eine Entschädigung für Fraport's Investitionen in Höhe von ca. 300 Mio. USD ergebnislos verlaufen waren. Die Klage von Fraport wurde aber mit der Begründung abgewiesen, dass der deutsch-philippinische Investitionsschutzvertrag nur solche Vermögenswerte schütze, die mit dem lokalen Recht in Einklang stehen. Die Philippinen hatten argumentiert, dass Fraport's Beteiligung an PIATCO gegen philippinisches Recht verstoße, weil Fraport direkt und indirekt 61% der Anteile an PIATCO halte. Dieser Einfluss sei teilweise durch gegenüber der philippinischen Regierung lange geheimgehaltene Kontrollabkommen zustande gekommen. Zulässig seien aber nur maximal 40%. Fraport habe dies zwar gewusst, den erhöhten Einfluss aber für notwendig gehalten, um die notwendige Kontrolle über seine erheblichen Investitionen zu gewinnen. Fraport's Investitionen seien daher nicht in „accordance with law" erfolgt, und das Schiedsgericht hat sich somit als nicht zuständig erklärt.

Ähnliche Investitionsbeschränkungen bestehen in den meisten asiatischen Ländern, auch wenn insgesamt ein Trend zur Liberalisierung erkennbar ist. Schon beim Markteintritt sollten ausländische Investoren überlegen, wie sie damit umgehen. Umgehungsversuche über fragwürdige Treuhandlösungen sind dabei meistens keine gute Antwort; stattdessen sollte der regulatorische Rahmen richtig genutzt oder direkte Absprachen mit den zuständigen lokalen Behörden getroffen werden: damit lassen sich Beteiligungs- und andere Beschränkungen oftmals ganz oder auf ein akzeptables Maß reduzieren.

3. Korruption

International tätige deutsche Unternehmen dürfen das sich verschärfende rechtliche Umfeld für Korruptionsdelikte im In- und Ausland nicht ignorieren. Die Rechtslage hat sich für Unternehmen in Deutschland in den letzten Jahren fundamental geändert.[15] Die Bestechung ausländischer Amtsträger ist ebenso wie die Bestechung von Mitarbeitern privater Unternehmen in ausländischen Märkten inzwischen in vielen Ländern strafbar, und im Ausland gezahlte Bestechungsgelder sind in Deutschland steuerlich nicht mehr abzugsfähig. In Asien kommt Singapur und Hong Kong besondere Bedeutung zu, weil Bestechungshandlungen anders als in den meisten Nachbarländern dort konsequent verfolgt werden, und viele Unternehmen von diesen Standorten aus Entscheidungen für die ganze Region treffen.[16] Vertragsgestaltungen und geschäftliche Praktiken sind auf ihre globalen Auswirkungen zu überdenken und erforderlichenfalls neu zu regeln.

---

15 *Fietz/Weidlich,* RIW 2005, 423 ff.; *Sedemund*, DB 2003, 323 ff.

16 *Fietz /Weidlich*, RIW 2005, 362 ff.

3.1 Schmiergelder in Asien

Asien ist die größte Wachstumsregion weltweit. Die deutschen Exporte nach Asien-Pazifik sind in den letzten Jahren stark angestiegen und deutlich über dem Durchschnitt der gesamten deutschen Ausfuhren gewachsen. Der innerasiatische Handel erlebt seit gut 15 Jahren phänomenale Zuwachsraten. Allein in China sind seit Beginn der wirtschaftlichen Öffnung in 1978 mehr als 800 Mrd. US$ an ausländischen Direktinvestitionen geflossen und ein Ende dieses Booms ist gerade bei deutschen Unternehmen nicht in Sicht. Viele deutsche Unternehmen sind geschäftlich in ganz Asien tätig oder planen entsprechende Investitionen.

Vielfach kommen Unternehmen im Ausland jedoch nur „ins Geschäft", wenn sie Schmiergelder an Entscheidungsträger ihrer Geschäftspartner tätigen. Ein häufig anzutreffendes Beispiel ist die Zahlung von „kick-backs" an einen Einkaufsmitarbeiter, Geschäftsführer oder nicht selten auch den Firmeninhaber selbst, der überhöhte Lieferpreise akzeptiert und dafür im Gegenzug von dem Vertragspartner einen Teil des überhöhten Einkaufspreises persönlich zurückerhält. Bestechungsgelder sind in vielen Ländern Asiens an der Tagesordung und können bei öffentlichen Aufträgen bis zu 30 % der Auftragsumme oder mehr ausmachen. Ein Blick in die Korruptionsstatistiken zeigt, dass Singapur und Hong Kong neben Japan weltweit die einzigen asiatischen Länder unter den Nationen mit geringer Korruption sind. Singapur liegt danach deutlich vor und Hong Kong in etwa gleichauf mit Deutschland und der asiatischen Wirtschaftsmacht Japan. Am Ende der Skala finden sich dagegen viele asiatische Länder wie Indonesien, die Philippinen, Südkorea, Thailand und Malaysia, aber auch die beiden großen Wachstumsmärkte China[17] und Indien. Als besonders korruptionsanfällige Branchen gelten die Bauwirtschaft und die Waffenindustrie, doch sind Schmiergelder auch in der Öl- und Gasindustrie und in vielen verarbeitenden Industrien relativ weit verbreitet.

Singapur und Hong Kong ist es durch spezielle Programme und strenge Gesetze gelungen, die Korruption auf ihrem Gebiet deutlich einzudämmen und sich damit von ihren korruptionsgeplagten Nachbarstaaten abzuheben. Es ist kein Zufall, dass gerade diese Standorte in den vergangenen Jahren für ausländische Investoren besonders attraktiv waren und zugleich zum stabilen Standbein für Transaktionen in benachbarte Länder wurden. Inzwischen gibt es Anzeichen, dass weitere asiatische Länder ernsthafter gegen Korruption vorgehen.[18] Dies gilt beispielsweise für Malaysia oder China,[19] wo sich die politische Führung dem Thema sichtbar angenommen hat und es jüngst zu einer Reihe von Verhaftungen hochrangiger Amtsträger und Unternehmer im Zusammenhang mit Korruptionsvorwürfen kam.

---

17 *Hoffbauer*, Handelsblatt, 14. Feb. 2006, Korruption: Die Allmacht der Partei hat die Vetternwirtschaft in China wuchern lassen- jetzt erfasst sie auch den Privatsektor.

18 *Kleine- Brockhoff*, Korruptionsvorwürfe gegen Siemens in Indonesien, http://www.tagesspiegel.de/wirtschaft/Siemens-Korruption-Siemens;art975,2399634.

19 *Qiao*, Bestechung ist der falsche Weg, China Contact, 1/2007, S. 31; Siemens droht Korruptionsverfahren in China, http://www.spiegel.de/wirtschaft/0,1518,503682,00.html, 04. Sep. 2007.

3.2 Die strafrechtliche Ausgangslage in Deutschland

Die Bestechung ausländischer Amtsträger wird in Deutschland als Folge der OECD Anti-Korruptions-Konvention seit dem 15. Februar 1999 bestraft.[20] Darüber hinaus droht deutschen Firmen und deren Repräsentanten seit 1. September 2002 auch im privatwirtschaftlichen Sektor bei Bestechungshandlungen im Ausland eine strafrechtliche Verfolgung in Deutschland. Nach § 299 Abs. 2 Strafgesetzbuch (StGB) macht sich strafbar, „wer im geschäftlichen Verkehr zu Zwecken des Wettbewerbs einem Angestellten oder Beauftragten eines geschäftlichen Betriebes einen Vorteil für diesen oder einen Dritten als Gegenleistung dafür anbietet, verspricht oder gewährt, dass er ihn oder einen anderen bei dem Bezug von Waren oder gewerblichen Leistungen in unlauterer Weise bevorzugt". Die in der Vergangenheit kontrovers diskutierte Frage, ob damit auch Handlungen im ausländischen Wirtschaftsverkehr erfasst sind, wurde durch das Gesetz vom 22. August 2002 zweifelsfrei beantwortet. Aufgrund des neu eingefügten § 299 Abs. 3 StGB sind nun grundsätzlich alle bestechungsrelevanten Tatbestände auch im Ausland, sei es inner- oder außerhalb der Europäischen Union, erfasst.[21]

Die meisten Bestechungsfälle im privaten Sektor können in Deutschland strafrechtlich verfolgt werden, wenn der Täter Deutscher ist und die Tat am Tatort mit Strafe bedroht ist oder der Tatort keiner Strafgewalt unterliegt (§ 7 Abs. 2 Nr. 1 StGB). Die Vorschrift ermöglicht damit eine Bestrafung deutscher Täter in Deutschland, wenn am ausländischen Tatort eine dem § 299 StGB entsprechende Vorschrift zur Bestechung/Bestechlichkeit im Wirtschaftsverkehr in Kraft ist. Denkbar ist ferner eine Strafverfolgung gestützt auf § 7 Abs. 1 StGB, wenn die Tat im Ausland „gegen einen Deutschen" begangen wurde. Auch wenn die im Ausland begangenen Bestechungstat dort nicht unter Strafe steht und ein Deutscher dafür in Deutschland nicht verfolgt werden kann, sind Teilnahmehandlungen in Deutschland strafbar. Anstiftung oder Beihilfe etwa durch das Bereitstellen von Bestechungsgeldern im deutschen Mutterhaus für Auslandsgeschäfte eines deutschen Mitarbeiters kann verfolgt werden, da eine rechtswidrige, vorsätzliche Haupttat (§ 9 Abs. 2 StGB) nach neuer Rechtslage stets vorliegt.

3.3 Fazit

Vor dem Hintergrund der internationalen Bestrebungen zur Bekämpfung von Korruption und Geldwäsche, der wachsenden Zahl einschlägiger nationaler Strafgesetze und der zunehmenden Verfolgung von Korruptionsdelikten in vielen Ländern sollten global operierende Unternehmen dem Thema erhöhte Aufmerksamkeit widmen. Mit der Neuregelung des § 299 Abs. 3 StGB rücken auch Auslandssachverhalte verstärkt ins Blickfeld der deutschen Strafverfol-

---

[20] *Gildeggen*, Internationale Handelsgeschäfte, 2. Aufl. 2005, S. 240.

[21] *Schönke/Schröder-Heine*, Kommentar zum Strafgesetzbuch, 27. Aufl. 2006, § 299 Rn. 2.

gungsbehörden. Die ersten Ermittlungen der deutschen Justiz wegen Bestechung im Ausland laufen bereits. Diese Fälle werden zunehmen, nicht zuletzt aufgrund der Meldepflichten der Finanzbehörden. Es steht zu erwarten, dass die deutschen Finanzbehörden auch Auslandssachverhalte im Rahmen von Betriebsprüfungen vermehrt aufgreifen werden.

Die Korruptionsrisiken sind eindeutig: neben hohen Haftstrafen und empfindlichen Geldbußen kann es zu einer nationalen oder sogar internationalen Sperre des betroffenen Unternehmens beispielsweise für öffentliche Aufträge kommen. Darüber hinaus droht der Verlust staatlicher Kreditgarantien. Der allgemeine Imageverlust durch öffentlichkeitswirksame Hausdurchsuchungen und negative Presseberichterstattung ist vielmals nicht mit Geld aufzuwiegen. Ein Bestechungsskandal auch weitab des Mutterhauses kann im *global village* schnell zu *global news* werden. US-amerikanische Multinationals sehen sich bereits seit 1977 unter dem *Foreign Corrupt Practices Act* dem Risiko von Strafverfolgung führender Mitarbeiter, Reputationsverlust für das Unternehmen und den damit verbundenen Kosten ausgesetzt. Viele amerikanische Firmen haben dementsprechend seit geraumer Zeit detaillierte Verhaltensregeln („*Code of Conduct and Business Ethics*") für ihre Mitarbeiter. Auch deutsche Unternehmen und ihre Mitarbeiter sollten über die regionalen Gegebenheiten in Asien informiert sein, um neben einer etwaigen Strafverfolgung in Deutschland nicht in Konflikt mit den lokalen Strafgesetzen zu kommen. Vertragsgestaltungen und geschäftliche Praktiken sollten überdacht und erforderlichenfalls neu geregelt werden. Verantwortlichkeiten müssen deutlich gemacht und dokumentiert werden.

Der Bundesgerichtshof fordert in mehreren Urteilen[22] eine organisatorische Vorsorge. Ein Unternehmen kann sich vor Wissenszurechnung nur dann schützen, wenn es einen angemessenen Informationsfluss nachweisen kann, und im Schadensfall kann eine Entlastung durch gute Informationsorganisation und den Nachweis einer regelmäßigen Kontrolle und Schulung erfolgen.[23] Klare Konzerndirektive muss sein, dass Korruption an keiner Stelle und in keiner Form geduldet und unternehmensintern streng sanktioniert wird.

---

22 BGH v. 8.12.1989 – V ZR 246/87, DNotZ 1991, 122; BGH v. 2.2.1996 – V ZR 239/94, DNotz 1996, 986, 988.

23 Zur Errichung einer Compliance-Organisation *Hauschka*, ZIP 2004, 877 ff.

4. Beschäftigung von Mitarbeitern im Ausland

4.1 Arbeitnehmerentsendung

Vor allem in der Anfangsphase werden Schlüsselpositionen einer ausländischen Tochtergesellschaft regelmäßig durch Expatriates besetzt. Zu den Gründen zählen vor allem die Sicherung europäischer Qualitätsmaßstäbe und eine bessere Umsetzung der Unternehmensphilosophie des Mutterhauses.[24] Dazu werden häufig deutsche oder europäische Mitarbeiter ins Ausland entsandt. Im Vorfeld sollte eine sorgfältige Planung aller rechtlichen und persönlichen Angelegenheiten des Auslandseinsatzes erfolgen.[25]

Die Gestaltung der Arbeitsverträge entsandter Mitarbeiter richtet sich hauptsächlich nach der Dauer der Entsendung. Handelt es sich um einen kurzfristigen Auslandseinsatz, wird der deutsche Arbeitsvertrag meist um eine Entsendevereinbarung ergänzt. Im Falle eines langfristigen Auslandeinsatzes ruht in der Regel das deutsche Arbeitsverhältnis und es wird ein befristeter Arbeitsvertrag mit dem Unternehmen im Ausland abgeschlossen. Bei einem unbefristeten Auslandseinsatz schließlich wird das deutsche Arbeitsverhältnis typischerweise aufgehoben und als Folge des „Übertritts" ein Arbeitsverhältnis mit dem ausländischen Unternehmen eingegangen. In diesem Fall erhält der Mitarbeiter dann meistens keine Rückkehrgarantie mehr.[26]

In der Praxis finden sich vielfach Mischformen oder – sehr häufig anzutreffen – schlicht unklare oder unverbindliche Regelungen. Die Verhandlung eines Entsendevertrages sollte gerade aufgrund der erhöhten Komplexität der Rechtsbeziehungen zum Anlass genommen werden, eine übersichtliche und die aktuellen Gegebenheiten reflektierende Vertragsgrundlage zu schaffen. Zu den wichtigen Regelungspunkten gehören eine genaue Beschreibung von Position, Aufgabenbereich und ggf. Berichtspflichten; Bestimmungen zur Vergütung nebst etwaiger Auslandszulagen, Anpassungsregelungen bei Währungskursschwankungen und die Festlegung der Steuerpflichten im Gast- und/oder Entsendeland. Weiterhin sind besondere Klauseln hinsichtlich der Ausreise sowie zu regelmäßigen Familienheimflügen, zu den Rechten und Pflichten bei einer Versetzung und der anschließenden Rückkehr sowie zu Kündigungsfristen und sonstigen bei Beendigung des Arbeitsverhältnisses zu regelnden Fragen erforderlich.

---

24 *Kolvenbach/Hölzchen*, Nicht Jugend, Erfahrung zählt: Personalentsendungen nach Asien, China Contact, 10/2007, S. 47.

25 *Brandt*, Gold im Kopf oder Klotz am Bein: Wer nach China entsandt wird, braucht die volle Unterstützung durch das Mutterhaus – vor, während und nach dem Aufenthalt, ASIA BRIDGE, 4/2006, S.34.

26 *Braun/Gröne*, in: Henssler/ Braun, Arbeitsrecht in Europa, 2. Aufl. 2007; Deutsches IPR des Arbeitsrechts, Rn. 42.

Auch im Arbeitsrecht gilt zunächst das Prinzip der Vertragsautonomie, d.h. die Parteien können das Arbeitsverhältnis einem von ihnen gewählten Recht unterwerfen.[27] Überlagert wird eine solche Rechtswahl aber ggf. von zwingenden arbeitsrechtlichen Vorschriften des objektiven Vertragstatus. Schon dessen Bestimmung ist jedoch nicht ganz einfach: wurde kein besonderes Recht vereinbart, unterliegt der Arbeitnehmer grundsätzlich dem Recht des Staates, in dem er gewöhnlich seine Arbeit verrichtet, selbst wenn er vorübergehend in einen anderen Staat entsandt wurde. Bis zu welchem Zeitraum eine lediglich vorübergehende Entsendung vorliegt, ist zweifelhaft. Soweit der Einsatz im Ausland nicht auf Dauer angelegt ist und drei Jahre nicht überschreitet, dürfte der vorübergehende Charakter gewahrt sein, mit der Folge, dass aus deutscher Sicht deutsches Arbeitsrecht auf das Arbeitsverhältnis mit dem Heimatunternehmen Anwendung findet.[28]

Bei Arbeitsverträgen mit entsandten ausländischen Arbeitnehmern sollte – im Interesse beider Parteien – sorgfältig überlegt werden, ob nicht ausdrücklich deutsches oder ein anderes ausländisches Recht vereinbart wird. Bei entsprechendem Sachzusammenhang und mit gewissen Einschränkungen ist eine solche Rechtswahl bei ausländischen Arbeitnehmern aus Sicht der meisten ausländischen Rechtsordnungen regelmäßig zulässig.

Stets von besonderem Interesse ist die steuerliche Gestaltung einer Entsendung. Die individuelle Steuerlast kann oftmals durch verschiedene Gestaltungsmöglichkeiten verringert werden, etwa den Abschluss dualer Arbeitsverträge oder die Gewährung geldwerter Vorteile. Vor Umsetzung sollte dies jedoch sorgfältig bedacht und erforderlichenfalls Rat eingeholt werden. Die Steuererklärungen von *Expatriates* werden in vielen Ländern verstärkt geprüft und Fehler oder unterlassene Informationen können sehr kostspielige Konsequenzen haben. Die Steuerbehörden können Bußgelder bis zur doppelten Höhe der zu wenig gezahlten Steuern erheben, in Betrugsfällen kann das Bußgeld teilweise sogar bis zu drei- oder viermal so hoch sein. Häufige Fehler sind die unterlassene Angabe aller Sachleistungen wie insbesondere Pensionsbeiträge, Wohnungs- oder Schulzulagen und sonstige Zuschüsse.

4.2 Beschäftigung lokaler Arbeitnehmer

Viele Länder in Asien haben sehr arbeitnehmerfreundliche Gesetze, die teilweise in ihrer Komplexität kaum hinter den deutschen Regelungen zurückstehen. Außerdem gibt es zahlreiche lokale Praktiken, die aus deutscher Sicht sehr gewöhnungsbedürftig sind.

In **China** bestehen in der Praxis Einschränkungen für die direkte Rekrutierung von Mitarbeitern durch ausländisch investierte Gesellschaften (*Foreign Invested Enterprises*, kurz FIE). So kann für eine Anzeige zur Suche nach Arbeitnehmern beispielsweise die Genehmigung

---

27 *Reithmann/Martiny*, Internationales Vertragsrecht 5. Aufl. 1996, 5. Teil: Einzelne Vertragstypen V. Arbeitsvertrag, Rn. 1332.

28 *Braun/Gröne,* a.a.O., (FN 26).

der örtlichen Arbeitsbehörde vorgeschrieben sein.[29] Vielfach neigen FIEs deshalb dazu, Arbeitnehmer aus einer von den örtlichen Arbeitsbehörden getroffenen Bewerbervorauswahl auszusuchen. Anstellungsverträge mit chinesischen Arbeitnehmern müssen schriftlich abgefasst und der örtlichen Arbeitsbehörde binnen einen Monats nach Vertragschluss zur Zertifizierung vorgelegt werden. Falls das Schriftformerfordernis nicht eingehalten wird, entsteht ein faktisches Arbeitsverhältnis mit unbefristeter Dauer. Mit Blick auf die restriktiven Kündigungsvoraussetzungen ist diese Rechtsfolge eine gravierende Sanktion. Es ist daher üblich, mit den zuständigen Behörden bzw. Gewerkschaften einen Standardarbeitsvertrag abzustimmen. Darüber hinaus erstellen viele größere Unternehmen ein "Employee Handbook" mit Verhaltenspflichten und anderen ergänzenden Regeln zum Arbeitsverhältnis. Diese Bestimmungen können vor allem für verhaltensbedingte Kündigungen sehr wichtig werden und sollten sorgfältig mit den Standardarbeitsverträgen abgestimmt sein. Zweifelsfragen in Bezug auf das Arbeitsverhältnis werden grundsätzlich im Sinne des Arbeitnehmers entschieden, so dass auf klare Regelungen besonders geachtet werden muss. Wettbewerbsverbote oder ähnliche Regelungen zum Schutz des Arbeitgebers sind zulässig, unterliegen jedoch Einschränkungen (z. B. Zahlung einer Karenzentschädigung und Beschränkungen in zeitlicher, geographischer und branchenbezogener Hinsicht), die mit denen in westlichen Rechtssystemen vergleichbar sind. Ein nachvertragliches Wettbewerbsverbot darf maximal zwei Jahre betragen, und die zwingend zu zahlende Karenzentschädigung muss angemessen sein.

Indien hat mit die rigidesten Arbeitsgesetze der Welt, die etwa die Schließung eines defizitären Betriebes sehr erschweren können. In der Praxis gelingt ein Personalabbau dann meistens ohne größere Schwierigkeiten, wenn sich der Arbeitgeber mit den Gewerkschaften auf einen Sozialplan einigt oder individuelle Absprachen mit den betroffenen Mitarbeitern schließt. Für Unternehmen mit 100 oder mehr Arbeitnehmern schreibt das Gesetz jedoch eine vorherige Genehmigung durch die zuständige Behörde vor. In der Praxis wird die Genehmigung für die Schließung eines Werkes allerdings so gut wie nie erteilt.

5. Unklare Regelungen und falsche Strukturen

Bei Geschäftsaktivitäten im Ausland ist besonderes Augenmerk auf die Ausgestaltung von Verträgen zu legen. Dies gilt sowohl für die „großen“ Verträge wie Joint Venture- oder Gesellschaftsverträge als auch für die vermeintlich kleineren, „unwichtigeren“ wie beispielsweise Liefer- oder Handelsvertreterverträge. Falsche oder nicht eindeutige Regelungen können erhebliche Nachteile für ein Unternehmen mit sich bringen, die im Nachhinein nur noch schwer zu beseitigen sind.

[29] *Falder*, Neue Spielregeln im chinesischen Arbeitsrecht: Arbeitsvertragsgesetz tritt am 1. Januar 2008 in Kraft, China Contact, 9/2007, S. 33.

Im Rahmen eines **Joint Venture Vertrags**[30] ist stets auch eine angemessene Wettbewerbsklausel zu verhandeln. Dies gilt insbesondere dann, wenn die Mutterhäuser im Kerngeschäft miteinander konkurrieren und strategische Konflikte daher vorprogrammiert sind. Der ausländische Investor, der ja regelmäßig Know-How und Technologien beisteuert, wird ein großes Interesse daran haben, dass der lokale Partner diese nicht zum Aufbau eines konkurrierenden Geschäfts nutzt. Insbesondere auch für die Zeit nach Beendigung des Joint Ventures ist daher bei entsprechender Verhandlungsmacht eine angemessene Regelung zu treffen. Das Wettbewerbsverbot ist dabei häufig so ausgestaltet, dass der lokale Partner weltweit nicht in Wettbewerb zu dem gemeinsamen Joint Venture treten darf, wohingegen der ausländische Partner außerhalb des betreffenden Landes frei bleibt, konkurrierende Tätigkeiten auszuüben.

In manchen asiatischen Rechtsordnungen besteht allerdings nur ein begrenzter Spielraum für die Vereinbarung eines durchsetzbaren Wettbewerbsverbots. Die für den Verstoß gegen das Wettbewerbsverbot regelmäßig vertraglich festgelegten Vertragsstrafen sind insbesondere in Common Law-Ländern nur dann durchsetzbar, wenn das Wettbewerbsverbot angemessen ist und die Höhe der Vertragsstrafe einer ehrlichen Schätzung des tatsächlich eingetretenen Schadens (genuine pre-estimate of liquidated damages) entspricht.[31] Außerdem sollten Joint Venture Verträge auch immer praktikable Regelungen zur Lösung von Pattsituationen enthalten. Viele Kooperationen scheitern letztlich daran, dass im Vorfeld nicht genügend Augenmerk auf die Entschärfung von Konflikten gelegt wurde.

In **Indien** ist eine weitere Besonderheit zu beachten. Die indische Regierung will den indischen Partner davor schützen, dass der ausländische Investor weitere Joint Ventures im gleichen Geschäftsfeld in Indien eingeht. Gemäß Press Note No. 1 (2005)[32] muss der ausländische Investor hierzu regelmäßig die Genehmigung des zuständigen *Foreign Investment Promotion Board* (FIPB) einholen. Das FIPB wird diese Genehmigung jedoch nur erteilen, wenn der indische Partner seine Zustimmung erteilt hat. Es ist daher stets ratsam, sich bereits bei Abschluss des Joint Venture Vertrags ein so genanntes *No-Objection Certificate* von dem indischen Partner aushändigen zu lassen, welches dann bei Eintritt bestimmter Bedingungen von dem ausländischen Investor verwendet werden darf. Wenn sich der indische Partner diesem Wunsch verschließt, sollte an die Aufnahme einer so genannten "Conflict of Interest" Klausel in dem Joint Venture Vertrag gedacht werden, worin festgelegt wird, unter welchen Voraussetzungen der indische Partner einer weiteren Kooperation des ausländischen Partners in Indien zustimmen muss.

Bei Staaten des Common Law, unter anderem Indien und Singapur, besteht ferner die *parol evidence rule* (Vermutung der Vollständigkeit und Richtigkeit einer Urkunde) zu berücksichtigen. Diese auf englischem Recht basierende Regelung wurde beispielsweise in §§ 93, 94 des Singapore Evidence Act verankert und schreibt die Wortlautauslegung eines Schriftstückes vor. Im Gegensatz zum deutschen und anderen Zivilrechtssystemen, in denen der wirkliche Wille der Parteien zu erforschen ist, werden mit einigen Ausnahmen äußere Umstände,

---

30 *Döser*, Vertragsgestaltung im internationalen Wirtschaftsrecht, 2001 S. 186.

31 Dunlop Pneumatic Tyre Co versus New Garage and Motor [1915] AC 79.

32 Press Note 1 (2005 Series) vom 12. Januar 2005.

die dem Wortlaut des schriftlichen Vertrages widersprechen oder ihn abändern, nicht berücksichtigt. Auch deshalb sollten Verträge in diesen Ländern besonders umfassend und sorgfältig gestaltet werden.

Bei **Handelsvertreterverträgen**[33] wird oftmals übersehen, dass der ansonsten zwingend vorgesehene Ausgleichsanspruch eines Handelsvertreters vertraglich ausgeschlossen werden kann, wenn der Handelsvertreter seine Tätigkeit für den Unternehmer außerhalb der Europäischen Gemeinschaft oder des EWR erbringt.[34] Dies ist beispielsweise der Fall, wenn ein in Deutschland ansässiges Unternehmen einen Handelsvertreter in Singapur mit der Betreuung der Geschäfte im asiatisch-pazifischen Raum beauftragt. Das deutsche Unternehmen kann hierbei den gesetzlich vorgeschriebenen Ausgleichsanspruch des Handelsvertreters abbedingen und so eine Zahlung bei Beendigung des Vertragsverhältnisses vermeiden. Voraussetzung für diese Rechtsfolge ist allerdings eine hinreichend klare vertragliche Regelung und eine Prüfung, ob lokale Gesetze dem möglicherweise entgegenstehen.

Darüber hinaus sollte auch bei **wirtschaftlich zusammenhängenden Verträgen** darauf geachtet werden, dass diese konsequent ausgestaltet und aufeinander abgestimmt sind. Dies gilt insbesondere für die Rechtswahl und die Vereinbarung einer Schiedsklausel. Zwar lässt sich aufgrund zwingenden Rechts nicht immer durchgehend eine Rechtsordnung für alle Verträge vereinbaren, insbesondere dann nicht, wenn nicht alle Verträge einen Bezug zu dem Land aufweisen, dessen Rechtsordnung gewünscht ist. Dennoch sollte in diesen Fällen, soweit möglich, zumindest eine einheitliche Schiedsklausel vereinbart werden. Dies gilt vor allem vor dem Hintergrund, dass sich eine Auseinandersetzung zwischen Vertragsparteien über einen bestimmten Vertrag oftmals auch auf andere, wirtschaftlich zusammenhängende Verträge zwischen den gleichen Parteien oder mit den Parteien verbundene Unternehmen ausdehnt. Verfahren vor mehreren Schiedsgerichten in unterschiedlichen Ländern, womöglich noch in verschiedenen Verfahrenssprachen, erschweren die Lösung der Auseinandersetzung erheblich und verursachen hohe Kosten.

6. Durchsetzung von Rechten

Die Durchsetzung von Rechten ist in vielen Ländern, vor allem außerhalb Europas, immer noch schwierig. Die Rechtssysteme vieler Schwellenländer entsprechen noch nicht dem westlichen Standard, hinzu kommt oftmals eine Überlastung der örtlichen Gerichte und / oder eine mangelnde Qualifizierung der Richter. Recht bekommen ist hier vor allem eine Frage des praktischen Vorgehens und der ausreichenden (vertraglichen) Vorsorge.

---

33 *Gildeggen*, a.a.O. (FN 20).

34 § 92c HGB.

6.1 Rechtswahl

Verträge können in vielen asiatischen Ländern grundsätzlich einer anderen als der lokalen Rechtsordnung unterstellt werden. Hierbei ist jedoch zu beachten, dass eine solche Rechtswahl oftmals nur dann wirksam ist, wenn sie bona fide, also in „gutem Glauben" bzw. ohne betrügerische Absicht erfolgt. Insoweit ist grundsätzlich erforderlich, dass eine gewisse Beziehung zu der gewählten Rechtsordnung besteht. Bei Verträgen zwischen lokalen und ausländischen Parteien ist allerdings regelmäßig auch die Wahl einer „neutralen" Rechtsordnung zulässig, auch wenn keine der Parteien oder der Gegenstand des Verfahrens dem gewählten Rechts zuzuordnen ist.[35]

6.2 Prozessrisiken

Asiatische Geschäftspartner vertreten ihre Position regelmäßig mit allem Nachdruck und mit Raffinesse. Es bestehen im Vergleich zu Europa noch immer fundamentale Unterschiede in der Art der Verhandlungsführung, und selbst ein unterzeichneter Vertrag wird nicht selten wieder in Frage gestellt. Auch können sich ausländische Investoren bisweilen unakzeptablen Ansprüchen von Geschäftspartnern ausgesetzt sehen oder – aufgrund ihrer Geschäftsverbindung mit einem lokalen Partner – überraschend in einen Rechtstreit mit ihnen unbekannten Dritten involviert werden. Das Prozessrisiko ist in manchen asiatischen Ländern recht hoch und Streitigkeiten werden sich häufig nicht vermeiden lassen. Ausländischen Investoren ist anzuraten, Verhandlungsergebnisse bestmöglich zu dokumentieren und das *worst case scenario* eines späteren Rechtsstreits schon beim Geschäftsabschluss einzuplanen. Vertraglich fixierte Schadensersatzsummen in bestimmter Höhe (*liquidated damages*) können ein wirksames Instrument zur Sicherung von Ansprüchen sein. In Joint-Venture-Verträgen sollte einer möglichen vorzeitigen Beendigung der Kooperation durch Ausstiegsklauseln (*exit clauses*) gebührende Beachtung geschenkt werden.

6.3 Gerichtssysteme

Viele asiatische Gerichtssysteme lassen noch immer zu wünschen übrig. Viele Richter sind noch zu unerfahren, um die Komplexität moderner Geschäftsabläufe ausreichend würdigen zu können. Der Ausgang eines Gerichtsverfahrens ist immer ungewiss, aber für **China**[36] gilt

---

[35] *Reithmann/Martiny* a.a.O. (FN 27) Rn. 54.

[36] *Glück/Semler*, RIW 2006, 436 ff.

dies wegen der fehlenden Tradition einer unabhängigen Gerichtsbarkeit wohl in besonderem Maße. Ohne Kenntnis der Umstände eines jeden Falles lassen sich nur schwer Schlussfolgerungen ziehen, doch gibt es leider zahlreiche Belege für Entscheidungen, die rational nicht nachvollziehbar sind oder in denen Gesetze widersprüchlich angewendet wurden. Nicht nur die Verteidigung gegen eine Klage, auch die gerichtliche Durchsetzung eines Anspruchs stellt sowohl für ausländische wie für einheimische Unternehmen oft ein erhebliches Problem dar. In China sollte der Kläger daher versuchen, sich die Regelungen zur örtlichen Zuständigkeit der chinesischen Gerichte zunutze zu machen, um beispielsweise den allgemeinen Gerichtsstand eines chinesischen Beklagten zu umgehen. Durch den vertraglich vorgesehenen Erfüllungsort lässt sich möglicherweise der grundsätzlich erforderliche Bezug einer Sache zum Gerichtsbezirk eines erfahrenen Gerichts (wie in Shanghai, Peking oder auch in Hong Kong) herstellen. Viele in China hergestellte Waren gelangen über Hong Kong in den Weltmarkt, so dass Beschlagnahmen und andere Maßnahmen einstweiligen Rechtsschutzes in der ehemaligen britischen Kolonie stets in Betracht gezogen werden sollten.

6.4 Schiedsverfahren

Bedenken hinsichtlich der Geschwindigkeit und Unparteilichkeit von asiatischen Gerichten bestehen nicht nur bei ausländischen Investoren, sondern sind manchmal auch in der lokalen Gesellschaft verbreitet. Die meisten Verträge zwischen lokalen und ausländischen Unternehmen enthalten deshalb Schiedsklauseln, die Streitigkeiten an Schiedsgerichte verweisen (und den Weg zu den ordentlichen Gerichten zunächst verschließen sollen). Den Parteien ist es grundsätzlich freigestellt, Vereinbarungen zur Schiedsgerichtsbarkeit zu treffen. Sie können hierzu Schiedsverfahren in oder außerhalb des jeweiligen Landes bestimmen und auch die vorherige Durchführung eines Vermittlungsverfahrens (Mediation) vorsehen. In der Vergangenheit wurden auch wirksam vereinbarte Schiedsgerichtsklauseln bisweilen von chinesischen Gerichten für unwirksam erklärt.[37] In der Praxis sollten möglichst die Musterschiedsklauseln der Internationalen Handelskammer (ICC) in Paris oder anderer anerkannter Schiedsorganisationen verwendet werden. Überhaupt ist bei der Abfassung der Schiedsklauseln höchste Sorgfalt geboten.[38]

Ein inländisches Schiedsurteil kann in den meisten Ländern Asiens durchgesetzt und vollstreckt werden.[39] Einwände gegen die Vollstreckung können nur unter ganz bestimmten Umständen geltend gemacht werden. Ein solches Vollstreckungshindernis stellt z. B. die Verlet-

---

37 Nach *Trappe*, SchiedsVZ 2006, 258, 263 mit Verweis auf Art. 58 Arbitration Law steht in China der Weg zum Gericht zur Klärung der Wirksamkeit der Schiedsvereinbarung stets offen. Ist am Schiedsort das Fehlen einer wirksamen Schiedsvereinbarung festgestellt worden, so ist diese Feststellung auch für das deutsche Exequaturgericht bindend, sofern sie anerkennungsfähig ist, vgl. hierzu *KG Berlin*, v. 18.5. 2006 – 20 Sch 13/04 (unveröffentlicht); *Kröll*, NJW 2007, 743, 749.

38 http://www.iccwbo.org.

39 Für China *Trappe*, SchiedsVZ 2006, 258, 268.

zung von Verfahrensvorschriften dar. Auch ist das Schiedsurteil dann nicht vollstreckbar, wenn der Streitgegenstand nicht schiedsgerichtsfähig war. Die Vollstreckung ausländischer Schiedsurteile richtet sich neben den jeweiligen lokalen Gesetzen vor allem nach den New Yorker und Genfer Abkommen zur gegenseitigen Anerkennung ausländischer Schiedssprüche, die sowohl Deutschland als auch eine Vielzahl der asiatischen Länder unterzeichnet haben. Ein in Einklang mit diesen internationalen Übereinkommen erlassenes ausländisches Schiedsurteil ist für die beteiligten Parteien bindend und wird von den lokalen Gerichten grundsätzlich anerkannt. Die im Schiedsverfahren obsiegende Partei muss bei dem sachlich und örtlich zuständigen Gericht im jeweiligen Land einen Antrag auf Vollstreckung des ausländischen Schiedsurteils stellen.

Die Vollstreckung ausländischer Gerichtsurteile ist im Vergleich zu Schiedsurteilen insbesondere in Common Law-Ländern wie Indien oder Singapur dagegen schwieriger. Für deutsche Gerichtsurteile muss oftmals ein eigenes Gerichtsverfahren angestrengt werden, in dem das deutsche Urteil mit gewissen Erleichterungen nochmals erstritten werden muss. Die Vereinbarung eines (in- oder ausländischen) Schiedsverfahrens ist auch vor diesem Hintergrund meist vorzugswürdig.

6.5 Investitionsschutz

Ausländische Investoren können, was oft nicht beachtet wird, Rechtsschutz möglicherweise auch aufgrund von Investitionsschutzabkommen erhalten.[40] Solche Investitionsschutzabkommen[41] hat Deutschland mit mehreren asiatischen Ländern unterzeichnet, unter anderem mit Indien und China. Diese zwischenstaatlichen Verträge bieten ausländischen Investoren Schutz für den Fall diskriminierender Maßnahmen von Seiten staatlicher Behörden und erlauben es, Schadensersatz direkt vor internationalen Schiedsgerichten einzufordern. Streitigkeiten werden im Regelfall an das International Centre for the Settlement of Investment Disputes (ICSID) in Washington verwiesen (unter Umständen mit Vorrang auch vor ausschließlichen Zuständigkeitsklauseln in einem Vertrag). Die Besonderheit von Investitionsschutzabkommen besteht darin, dass der Gang zu einem Schiedsgericht auch dann möglich ist, wenn in den Vereinbarungen der Parteien selbst keine Schiedsklausel enthalten ist. Die Investitionsschutzabkommen enthalten ein Angebot des Vertragsstaates, sich auf ein Schiedsverfahren einzulassen, das von einem Investor – der selbst nicht Partei des Schutzabkommens ist – im Streitfall durch die Einreichung einer Schiedsklage stillschweigend angenommen wird.[42]

---

40 Hierzu ausführlich *Wegen/Raible*, SchiedsVZ 2006, 225 ff.

41 Freshfields Bruckhaus Deringer, Effektiver Rechtsschutz bei Auslandsinvestitionen: Bilaterale Investitionsschutzabkommen, Mai 2007.

42 *Happ*, IStR 2006 Heft 19, 649; *Freudenberg*, Firmen im Ausland nicht schutzlos, Handelsblatt, 14. Juni 2006.

7. Erfahrungen aus der Transaktionsberatung

Im Vorfeld einer Akquisition oder gegebenenfalls auch anderer Investitionen wie eines Joint Ventures sollte in jedem Land regelmäßig eine ausführliche **Due Diligence** des Zielunternehmens bzw. des lokalen Partners durchgeführt werden. In Common Law-Ländern wie Indien oder Malaysia ist dies insbesondere schon deshalb erforderlich, weil dort das sog. Caveat-Emptor Prinzip gilt, nach welchem es im Verantwortungsbereich des Käufers liegt, den Kaufgegenstand vor dem Erwerb zu untersuchen. Die Due Diligence sollte dabei möglichst multidiziplinär ausgestaltet sein, also rechtliche, steuerliche, finanzielle und andere Aspekte abdecken. Die Schwerpunkte der rechtlichen Due Diligence liegen typischerweise in Bereichen wie *Corporate Compliance*, Grundbesitz, *Change-of-Control-* Klauseln, Rechtsstreitigkeiten und Verbindlichkeiten allgemein, Beziehungen mit verbundenen Unternehmen bzw. Personen sowie im Bereich des Arbeitsrechts.

In vielen Schwellenländern stellt bereits die Due Diligence eines Zielunternehmens große Herausforderungen an den ausländischen Investor, wobei ein pragmatisches Vorgehen angezeigt ist. Viele wichtige Informationen sind bei privaten Unternehmen oft überhaupt nicht oder bestenfalls oberflächlich und unvollständig dokumentiert und nur schwer zu erhalten. Bilanzen und juristische Dokumente entsprechen nicht immer internationalen Standards. Gespräche mit dem Management des Zielunternehmens, mit Firmenangehörigen und den lokalen Behörden sind deshalb häufig die wichtigste Quelle, um Informationen zu erlangen. Zugleich sollten sich Investoren aber nicht unkritisch auf die Äußerungen der lokalen Seite bei einer Transaktion verlassen, auch wenn ein staatliches Unternehmen beteiligt ist. Auch aus diesen Gründen dauern Due Diligence Untersuchungen in Asien meist deutlich länger als bei Targets im Westen. Das unübersichtliche Dickicht an Regularien erlaubt z. B. indischen Unternehmen eine Vielzahl an rechtlichen und steuerlichen Gestaltungsmöglichkeiten, die nur vor dem Hintergrund auch informeller Praktiken in Indien zu verstehen sind.

M&A-Transaktionen müssen in vielen asiatischen Ländern grundsätzlich von einer oder mehreren zuständigen Behörden genehmigt werden. Die staatlichen Stellen haben so erheblichen Einfluss auf Zustandekommen und auch Inhalt eines M&A-Deals.

Die für eine M&A-Transaktion zu beachtenden Vorgaben divergieren in Asien sehr stark. Es gibt in **China** zum Beispiel eine Reihe spezifischer M&A Regelungen für bestimmte Erwerbskonstellationen.[43] Die einschlägigen Regelungen sind jedoch nicht sehr übersichtlich und zudem stetem Wandel unterworfen. Zum Beispiel ist es nicht immer klar, welche Rechtsvorschriften auf die Zielgesellschaft anwendbar sind, nachdem der ausländische Investor eingestiegen ist. Je nach Zielunternehmen und Beteiligungsart gibt es verschiedene Möglich-

[43] *Fischer*, Neue Verordnung für Übernahmen, ASIA BRIDGE, 10/2006, S. 35; *Ben QI*, China's New M&A Rules: A Revisionist´s View, asialaw M&A Review, S. 23.

keiten, ein Unternehmen in China zu erwerben.[44] Ausländische Investoren sollten sich außerdem darüber im Klaren sein, dass eine Vielzahl von Zustimmungen und Genehmigungen erforderlich werden können, etwa solche von Aktionären, den Behörden und in einigen Fällen sogar von den Kreditgebern. In China bestehen üblicherweise bis zu einem gewissen Grad Unsicherheiten über das Vermögen und die Verbindlichkeiten der zur Übernahme ins Auge gefassten Gesellschaft. Ein ausländischer Investor sollte daher auch in Gespräche mit den Gläubigern des Zielunternehmens eintreten und diese in den Verhandlungsprozess einbeziehen, um sicher zu gehen, dass er einen richtigen Eindruck von der Vermögenssituation des Unternehmens erhält.

In einigen asiatischen Ländern muss der Kaufpreis grundsätzlich innerhalb eines bestimmten Zeitraumes nach dem Erwerb gezahlt werden, so dass die im internationalen Transaktionsgeschäft üblichen so genannten Earn-Out-Regelungen, nach denen ein Teil des Kaufpreises von den Ergebnissen der Zielgesellschaften abhängig und auch erst nach Ablauf der jeweiligen Geschäftsjahre zur Zahlung fällig ist, nicht vereinbart werden können. Solche *Earn-Out-Regelungen* dienen dazu, den Verkäufer für einen Übergangszeitraum weiterhin an dem Unternehmen zu beteiligen, damit dieser die reibungslose Integration und Fortsetzung des Unternehmens unterstützt. Alternativen zu einer *Earn-Out-Klausel* sind die Verpflichtung des Verkäufers zu entgeltlichen Unterstützungsleistungen oder zur Gewährung eines Darlehens zugunsten der Zielgesellschaft über einen Teil des Kaufpreises, solange die im Anteilskaufvertrag festgelegten Gewährleistungsfristen laufen. Hierbei ist jedoch zu beachten, dass solche Darlehen z. B. in China zwingend über eine Bank abgewickelt werden müssen, da direkte Darlehen zwischen Gesellschaften unzulässig sind.

Weiterhin besteht regelmäßig ein Interesse des Erwerbers, das Management des Zielunternehmens zumindest für die Anfangszeit beibehalten zu können. Hierzu dienen *Lock in*-Klauseln. Ob diese jedoch auch im jeweiligen asiatischen Land durchgesetzt werden können, ist anhand des lokalen Arbeitsrechts, das beispielsweise in China auch auf Geschäftsführer Anwendung findet, genau zu prüfen. Möglicherweise steht der Wirksamkeit solcher Klauseln das örtliche Kündigungsrecht im Weg.

Eine wichtige Rolle spielen neben den harten Assets und dem Management auch die Mitarbeiter der Zielgesellschaft, die den Wert eines Unternehmens aufgrund ihrer Expertise und ihres Know-How erheblich mit beeinflussen. Unerlässlich ist hier eine reibungslose Kommunikation und Information bereits während der Transaktion, um eventuell bestehende Unsicherheiten oder Missverständnisse auf Seiten der Arbeitnehmer zu beseitigen sowie die Schaffung von Anreizen, um wichtige Mitarbeiter nach der Transaktion zu halten. In vielen asiatischen Ländern sind die Interessen der Mitarbeiter gesetzlich zu beachten. Soweit z. B. in **China** die Arbeitnehmer der beteiligten Unternehmen gewerkschaftlich organisiert sind, sollten vor der Entscheidung über eine Fusion ihre Vertreter gehört und ihre Ansichten berücksichtigt werden. Kommt es in Folge der Übernahme zu Entlassungen, sind sowohl staatliche als auch lokale Vorschriften zu beachten. Regelmäßig werden an die zu entlassenden

---

44 *Tang/Ghaffar*, M&A- Transaktionsstrukturen in China – aktuelle Entwicklungen, Perspektiven, Frankfurter Allgemeine Buch, 2006, S. 154.

Arbeitnehmer Abfindungen zu zahlen sein. Bei der Übernahme eines chinesischen Unternehmens ist ein Sozialplan für die Arbeitnehmer aufzustellen und durch die Gewerkschaft genehmigen zu lassen. Bei der Fusion mehrerer ausländisch investierter Unternehmen besteht in China die Pflicht, sich um die Übernahme der gesamten Belegschaft oder eine sozialverträgliche Lösung zu bemühen. Auch bei Unternehmensübernahmen wird von den chinesischen Behörden oftmals auf ein solches Ergebnis hingewirkt.

Rechtliche Aspekte von IT-Compliance

Michael Rath

Zusammenfassung

Sowohl Corporate Governance (die verantwortungsvolle Steuerung des Unternehmens) als auch Corporate Compliance (die Umsetzung der notwendigen Kontrollmaßnahmen) sind angesichts der stetig zunehmenden Komplexität von Geschäftsprozessen in einem Unternehmen heutzutage ohne den Einsatz von Informationstechnologie (IT) nicht mehr vorstellbar. Corporate Governance und Compliance sind daher untrennbar mit IT-Compliance, dem verantwortungsvollen Umgang mit allen Aspekten von IT, verbunden. IT-Compliance reicht von der Etablierung eines (am besten IT-gestützten) Informations- und Kontrollsystems (IKS) und der Einhaltung von Datenschutz und Datensicherheit über die Sicherstellung von IT-Security bis hin zur gesetzeskonformen elektronischen Archivierung. Dieser Beitrag soll einen ersten Überblick über die große Bandbreite von IT-Compliance bieten.

1. Einleitung

Der vor allem gesellschaftsrechtlich geprägte Begriff der „Corporate Governance“ wird häufig umschrieben mit „verantwortungsvoller Unternehmenssteuerung durch die Geschäftsführung“. Danach sind sowohl der Vorstand einer AG als auch der Geschäftsführer einer GmbH als eigentliche Adressaten der Corporate Governance verpflichtet, neben der Einhaltung von einschlägigen Gesetzen für eine transparente Organisation und ein angemessenes Risikomanagementsystem zu sorgen. Diese Governance wird erreicht durch Compliance, vorliegend verstanden als die Gesamtheit aller organisatorischen Aufsichts-, Schulungs- und Kontrollmaßnahmen der Geschäftsleitung (einschließlich der Einrichtung eines Berichts- und Dokumentationswesens), welche einen Verstoß des Unternehmens gegen gesetzliche Pflichten verhindern sollen.

Corporate Governance und Compliance sind wegen der stetig zunehmenden Komplexität von Geschäftsprozessen in einem Unternehmen untrennbar mit IT-Compliance verknüpft. Dabei sind die Sicherstellung von IT-Compliance und der Gedanke der Beherrschung von IT-Risiken durch Risikoidentifikation, Risikoanalyse, Risikobewertung und Risikosteuerung bezüglich der im Unternehmen vorhandenen IT nicht neu.[1] Vielmehr gehört es angesichts der stetig wachsenden Bedeutung der IT für ein Unternehmen schon seit geraumer Zeit zu der verantwortungsvollen Steuerung eines Unternehmens, auch im Hinblick auf die vorhandene (oder etwa neu anzuschaffende) Informationstechnologie die geltenden „Spielregeln" einzuhalten und aktiv ein IT-Sicherheits- und Risikomanagement zu betreiben.

2. IT-Compliance als Aufgabe des Management

IT-Compliance ist keine Aufgabe, die allein von der IT-Abteilung oder dem CIO bewältigt werden kann. Zur Vermeidung einer (persönlichen) Haftung des Vorstandes oder des Geschäftsführers nach §§ 93 Abs. 2, 116 Abs. 1 AktG (analog), 43 GmbHG ist vielmehr gerade das Management aufgerufen, sich um die Einhaltung von IT-Compliance zu bemühen. Für die Unternehmensleitung folgt dies bereits aus den allgemeinen Sorgfaltspflichten.

Die Verpflichtung der Geschäftsleitung zur Sicherstellung von IT-Compliance ist nach diesem Verständnis also auch im Gesetz niedergelegt. Nach § 93 Abs. 1 AktG haben die Vorstandsmitglieder bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Angesichts der Bedeutung von IT für das Funktionieren und den Fortbestand des Unternehmens gehört es damit zu den Pflichten eines gewissenhaften Geschäftsführers, das Unternehmen vor erkennbaren Gefahren zu schützen. Verletzt ein Vorstand diese Pflicht, haftet er dem Unternehmen nach § 93 Abs. 2 AktG. Nach Satz 2 kommt es sogar zu einer Beweislastumkehr zu Lasten des Vorstandes einer Aktiengesellschaft, denn den Geschäftsleiter trifft die Beweislast hinsichtlich der Anwendung der geboten Sorgfalt. Das Management muss also nachweisen können, dass auch im Zusammenhang mit der IT die erforderliche Sorgfalt Anwendung gefunden hat. Diese im Aktienrecht für Vorstände festgelegten Pflichten gelten kraft entsprechender Regelungen (etwa §§ 43 GmbHG, 347 HGB) auch für den Geschäftsführer einer GmbH oder die Geschäftsleitung von OHGs und KGs. Der Bedeutung der IT für das Unternehmen entspricht es, dass gem. §§ 289, 317 HGB auch im Lagebericht der Gesellschaft Angaben zu den vorhandenen Risikofrüherkennungs- und IT-Systemen zu machen sind.

1 Siehe zu IT-Risiko und Chancenmanagement im Unternehmen den gleichnamigen Leitfaden der Bitkom, abrufbar unter http://www.bitkom.org/files/documents/Bitkom_Leitfaden_IT-Risikomanagement_V1.0_final.pdf.

Obwohl mithin der primäre Adressatenkreis von Compliance die Unternehmensleitung ist, werden Vorstand, Aufsichtsrat und Geschäftsführer oft versuchen, die Aufgaben betreffend die Einhaltung von IT-Compliance (zumindest teilweise) zu delegieren. Leitende Mitarbeiter des Unternehmens haften jedoch auch dann, wenn IT-Compliance kraft Weisung oder arbeitsvertraglicher Regelung zum Bestandteil des Pflichtenkataloges des IT-Administrators, Datenschutzbeauftragten oder des CIO gemacht werden.

3. Anforderungen von IT-Compliance

Die Schwierigkeit, die große Bandbreite von IT-Compliance überschaubar darzustellen, liegt schon allein darin begründet, dass die einschlägigen Vorgaben in einer Vielzahl von Gesetzen, Richtlinien und gegebenenfalls sektorspezifischen Anforderungen enthalten sind. Weltweit soll es schätzungsweise über 25.000 Compliance-Anforderungen (im weiteren Sinne) geben.[2] Auch wegen der oftmals völlig unterschiedlichen Zielrichtungen einschlägiger Normen ist es schwierig, die wesentlichen Eckpunkte von IT-Compliance zu benennen. Demgemäß sollen nachfolgend nur einzelne bedeutsame Aspekte von IT-Compliance hervorgehoben werden; die vorliegende Darstellung erhebt keinerlei Anspruch auf Vollständigkeit.[3]

Die Einhaltung von IT-Compliance wird zudem dadurch erschwert, dass aus ganz anderen Fachrichtungen, etwa dem Steuerrecht und der Wirtschaftsprüfung, weitere Anforderungen an die IT gestellt werden. Zudem gibt es neben den eher generischen gesetzlichen Regelungen in der Abgabenordnung (AO) und den Prüfungskatalogen der Wirtschaftsprüfer auch konkrete behördliche Vorgaben, etwa der Finanzverwaltung und der BaFin.

---

2 Vgl. bzgl. der Anforderungen von Solvency II etwa *Pfeifer*, VW 2005, 1558 ff.; bzgl. der Eigenkapitalvereinbarung Basel II siehe etwa *Duisberg/Ohrtmann*, ITRB 2005, 160 ff.

3 IT-Compliance kann vielmehr beispielsweise auch im Arbeitsrecht Bedeutung erlangen, so etwa hinsichtlich der Mitspracherechte des Betriebsrates (§ 80 BetrVG) bei der Einführung von bestimmten IT-Systemen (insbesondere von Programmen mit Überwachungsfunktionen) sowie bei so scheinbar trivialen Aspekten wie der Einhaltung der Bildschirmarbeitsplatzverordnung.

3.1 IT-gestütztes Informations- und Kontrollsystem (IKS)

Ein überaus wesentlicher Aspekt von IT-Compliance ist zunächst die Einhaltung von gesetzlichen Anforderungen und Informations- sowie Dokumentationspflichten *mit Hilfe der IT*. Es ist mitnichten nur aus betriebswirtschaftlicher und unternehmerischer Sicht wünschenswert, dass die im Unternehmen vorhandenen IT-Systeme in der Lage sind, über die Identifikation bestandsgefährdender Entwicklungen hinaus sämtliche Geschäftsvorfälle dauerhaft zu erfassen. Vielmehr dient eine solche Informationsgewinnung auch der Zusammenführung aller für unternehmerische Entscheidungen wichtigen Informationen. Aus diesem Grund wird auch vom Gesetzgeber eine effektive Kontrolle über die Prozesse im Unternehmen und die Einhaltung einer so verstandenen IT-Governance gefordert.[4]

Die gesetzliche Verpflichtung zur Einführung eines internen Kontrollsystems (IKS)[5] wurde durch das bereits am 1. Mai 1998 in Kraft getretene KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) eingeführt. Um eine angemessene wirtschaftliche Kontrolle und Transparenz in der AG und der GmbH zu erreichen, wurde durch das KonTraG insbesondere die Haftung von Vorstand und Aufsichtsrat erweitert. So wurde (wie bereits eingangs dargelegt) in § 91 Abs. 2 AktG bestimmt, dass der Vorstand geeignete Maßnahmen zu treffen und insbesondere ein Überwachungssystem einzurichten hat, damit etwaige den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden können. Ein zentraler Bestandteil ist dabei auch die Beurteilung der Angemessenheit und Wirksamkeit der IT-spezifischen Kontrollen als Teil des internen Kontrollsystems.

Das interne Kontrollsystem dient vor allem der Kontrolle von Fehlerrisiken. Fehlerrisiken setzen sich (übrigens nicht nur in der IT) zusammen aus „inhärenten Risiken“ und den „Kontrollrisiken“: Inhärente Risiken bezeichnen allgemein die Wahrscheinlichkeit für das Auftreten wesentlicher Fehler (etwa in der Rechnungslegung). Die Wahrscheinlichkeit dafür, dass wesentliche Fehler nicht rechtzeitig durch dieses interne Kontrollsystem aufgedeckt oder verhindert werden, wird allgemein als Kontrollrisiko bezeichnet.[6]

Daneben ist ein solches IKS aber auch deshalb erforderlich, um eine ausreichende Basis zur Unternehmenslenkung und zur Erfüllung von den einschlägigen gesetzlichen Berichts- und Dokumentationspflichten zu geben. Diese idealerweise in einem strukturierten „Business Information Warehouse“ gesammelten Informationen bilden dann die Grundlage der sog. „Business Intelligence (BI)“. Dieser Bestandteil von IT-Compliance wird daher teilweise auch als „Information Security Governance (ISG)“ oder „Management Risk Controlling (MRC)“ bezeichnet.

---

[4] Zu den künftigen Anforderungen von EURO-SOX siehe nachfolgend unter Ziffer 3.2.

[5] Zur Definition eines IKS siehe *Lösle/Maudrich*, DSWR 2006, S. 5 mit Hinweis auf IDW PS 260, Tz. 5.

[6] Zu den IT-bezogenen Kontrollen, deren Wirksamkeit die Basis für die Risikoeinschätzung bildet, zählen die allgemeinen IT-Kontrollen und die Anwendungskontrollen.

3.2 SOX & Co.

Ähnliche Anforderungen an die Etablierung und Aufrechterhaltung von Kontroll- und Informationssystemen (und damit mittelbar auch an die IT) enthält auch der im Zusammenhang mit dem Thema Compliance stets zitierte Sarbanes-Oxley-Act (kurz: SOX oder SOA).[7] Die Nichteinhaltung der Kontroll- und Dokumentationspflichten nach SOX-404, die nach der von der SEC gewährten Gnadenfrist (Geltung nur für Unternehmen mit Geschäftsjahresende nach dem 15. Juli 2006) nunmehr auch für nicht an der Stock Exchange notierte Tochtergesellschaften von US-amerikanischen Unternehmen gelten, wird streng sanktioniert: Abschnitt 802 des SOX sieht bei Zerstörung oder Veränderung von aufbewahrungspflichtigen Unterlagen drakonische Strafen vor (Strafmaß: bis zu 20 Jahren Gefängnis). Auch andere amerikanische Vorgaben wie bspw. HIPAA, Tread Act oder DoD 5015.2, können für deutsche Firmen mit Niederlassungen in den USA von Bedeutung sein. Es muss jedoch auch bei der Diskussion um IT-Compliance nochmals deutlich hervorgehoben werden, dass die Vorgaben des Sarbanes Oxley Act zunächst nur für US-amerikanische börsennotierte Unternehmen und deren ausländischen Töchtern gelten. Trotzdem ist in der Praxis die Tendenz feststellbar, dass auch in Verträgen mit deutschen Unternehmen, die gar nicht unmittelbar von SOX erfasst sind, die Einhaltung sämtlicher SOX-Vorgaben gefordert wird.

Section 404 enthält ausdrückliche Bestimmungen über Maßnahmen bezüglich der Errichtung eines internen Kontrollsystems (Management Assessment of Internal Controls). Secton 404 fordert dabei u.a., dass ein effektives internes Kontrollsystem zur Sicherstellung einer funktionsfähigen Berichterstattung eingerichtet wird. Ähnlich wie der Lagebericht deutscher Kapitalgesellschaften muss daher auch der Jahresbericht einer SEC-notierten Gesellschaft gemäß Section 404 einen Bericht des Managements („Internal Control Report“) über das vorhandene Kontrollsystem enthalten. Darin muss das Management u. a. Erklärungen hinsichtlich der Effizienz der eingerichteten Kontrollmaßnahmen abgeben, die dann auch gemäß Section 302 vom Vorstand im Rahmen der „Certification“ zu bestätigen sind. Zur Konkretisierung dieser Vorgaben hat das Committee of Sponsoring Organisations of the Treadway Commission (COSO) ein Rahmenkonzept entwickelt, dessen Anwendung von der SEC empfohlen wird. Das Kontrollmodell CobiT (Control Objectives for Information and Related Technology) lehnt sich eng an dieses COSO-Modell an (vgl. dazu noch nachfolgend im Rahmen der IT-Standards).

Mit der 8. EU-Richtlinie (sog. EURO-SOX oder Prüferrichtlinie) sollen zudem die internationalen Prüfungsstandards (ISA) europaweit verpflichtende Wirkung erhalten. Hierdurch werden aber u. a. auch strengere Anforderungen an die gesetzliche Abschlussprüfung bei Unternehmen öffentlichen Interesses (aus heutiger Sicht börsennotierte Unternehmen, Banken und Versicherungen, Energieversorger) gestellt. Neben neuen Regelungen für die Ab-

---

[7] Vgl. hierzu auch die Studie „Der Sarbanes-Oxley Act als Instrument der Corporate Governance“ (Juli 2006) der Detecon International GmbH, abrufbar unter www.detecon.com/de/publikationen/studien.

schlussprüfer wird die Einführung eines Prüfungsausschusses verpflichtend, das gleichsam wie das „Audit Committee“ im SOX die Aufgabe hat, die Abschlussprüfung sowie interne Kontrollsysteme und Risikomanagementsysteme zu überwachen.

Die Einrichtung von angemessenen Zugriffsberechtigungen bei IT-Systemen und entsprechenden Kontrollen ist seit SOX eine weitere Anforderung an die Buchführungssysteme. Die Unternehmensleitung muss danach (am besten mittels einer Echtzeitverarbeitung der unternehmensrelevanten Informationen) ausreichend über die tatsächlich im Unternehmen ablaufenden Prozesse – und nicht etwa die Soll-Prozesse – informiert sein und diese kontrollieren. Dies ist auch deshalb notwendig, da sonst etwaige Missstände erst viel zu spät (etwa im Rahmen einer aktienrechtlichen Sonderprüfung oder der Entscheidung über die Notwendigkeit einer Ad-hoc-Meldung) identifiziert würden. In einem großen Unternehmen kann aufgrund der großen Komplexität der im Unternehmen vorhandenen Prozesse ohnehin nur durch softwaregestützte Informationsmanagement-Prozesse und IT-gestützte Reportings sichergestellt werden, dass die unternehmerischen Entscheidungen auf der Grundlage angemessener Informationen getroffen werden. Es ist im Rahmen des zuvor beschriebenen allgemeinen Risikomanagement also auch notwendig, EDV-gestützte Maßnahmen zur Begleitung der Prozesse und zur Risikofrüherkennung zu etablieren und mit Hilfe der EDV auf ihre Brauchbarkeit hin zu kontrollieren.[8] Bei der Etablierung eines solchen „Governance, Risk and Compliance-Framework“ helfen Enterprise-Content-Management (ECM)-Lösungen. Solche ECM-Programme werden inzwischen – gerade auch mit Blick auf eine gesetzeskonforme Archivierung – zahlreich angeboten und helfen dem Unternehmen, den Überblick über die vorhandenen Informationen zu behalten.

3.3 Audit der IT-Systeme

Angesichts der Bedeutung von IT-Systemen für das Unternehmen versteht es sich fast von selbst, dass auch der Abschlussprüfer im Rahmen von (freiwilligen oder gesetzlich vorgeschriebenen) Jahresabschlussprüfungen gemäß § 317 Abs. 4 HGB die im Unternehmen vorhandenen Überwachungssysteme, also auch die dort etablierten Risikomanagement-Prozesse und zugehörigen Risikofrüherkennungs- und IT-Systeme zu beurteilen hat. Nach IDW PS 330 sind deswegen bei der Prüfung des IT-Systems Aufbau, Angemessenheit und Funktion des Risikomanagement zu beurteilen. Bei dieser Beurteilung hilft dem Prüfer u.a. die über 100 Fragen umfassende Checkliste zur Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PH 9.330.1).[9]

Die steigende Bedeutung der IT für Unternehmen verändert auch die Arbeit des Abschlussprüfers. Die Beurteilung der Ordnungsmäßigkeit der Rechnungslegung erfolgt heutzutage im zunehmenden Maße neben der beleghaften Prüfungsmethode auch indirekt über die Ord-

8 Zum Risikomanagement siehe *Bier*, K&R 2005, 59 ff.

9 Vgl. *Skopp/Greipl*, DSWR 2006, 2-4.

nungsmäßigkeit der IT-gestützten Buchführungsprozesse und die Wirksamkeit der IT-bezogenen Kontrollen. Demgemäß berücksichtigt auch der Prüfungsstandard (PS) 260 des Institutes der Wirtschaftsprüfer (IDW) die Bedeutung der IT-Landschaft als wesentliche Komponente des IKS.

Die Frage, wann die Abschlussprüfung zwingend eine IT-Prüfung zu umfassen hat, richtet sich insbesondere nach der Wesentlichkeit des IT-Systems für die Rechnungslegung bzw. für die Beurteilung der Ordnungsmäßigkeit der Rechnungslegung, der Komplexität des eingesetzten IT-Systems sowie dem Grad der Integration der EDV-Lösung. Die IT-Prüfung ist mittlerweile insbesondere bei mittelgroßen bis großen Unternehmen integraler Bestandteil einer Vielzahl von Jahresabschlussprüfungen und leistet für diese einen signifikanten Beitrag zur Erhöhung der Prüfungssicherheit. Diverse IDW-Stellungnahmen konkretisieren die Anforderungen an die Rechnungslegung aus Sicht der Wirtschaftsprüfer, so insbesondere die IDW RS FAIT 1 (Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie) und die IDW RS FAIT 3 (Grundsätze ordnungsmäßiger Buchführung bei Einsatz elektronischer Archivierungsverfahren). Auch bezüglich der Auslagerung von E-Commerce-Systemen gibt es eine IDW Stellungnahme zur Rechnungslegung (Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce, IDW RS FAIT 2).

3.4 IT-Security

Neben der bereits zuvor beschriebenen Verpflichtung des Vorstandes nach § 91 Abs. 2 AktG zur Schaffung eines internen Kontrollsystems (IKS) ist die Unternehmensleitung auch zur Etablierung effektiver IT-Sicherheitsmaßnahmen (sog. IT-Sicherheit oder IT-Security) und deren Kontrolle verpflichtet.[10] Diese Verpflichtung ergibt sich neben § 91 Abs. 2 AktG vor allem aus den allgemeinen Sorgfaltspflichten des Vorstandes, die in § 93 Abs. 1 AktG niedergelegt sind. Danach haben – wie zuvor gezeigt – die Vorstandsmitglieder bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Demgemäß ist die Unternehmensleitung auch zu einem angemessenen Risikomanagement hinsichtlich der vorhandenen IT-Systeme verpflichtet.

Die Verpflichtung zur Etablierung und Aufrechterhaltung von „IT-Sicherheit“ als ein weiterer Bestandteil von IT-Compliance bedeutet, dass die IT-Systeme (und die darin enthaltenen ggfls. sogar vertraulichen Informationen) gegen Angriffe von innen und außen geschützt werden müssen. Erläuternd kann man im Zusammenhang mit dem Begriff IT-Sicherheit auf eine Definition zurückgreifen, die im Zusammenhang mit der Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aufgestellt wurde. So heißt es in

[10] Siehe zu den rechtlichen Verpflichtungen zur Gewährleistung von IT-Security und zur Einführung einer Notfallplanung im IT-Bereich *Steger*, CR 2007, 137 ff.; *Heckmann*, MMR 2006, 280 ff.; *Roth/Schneider*, ITRB 2005, 19 ff.

§ 2 Abs. 2 BSIG, dass Sicherheit in der Informationstechnik die Einhaltung bestimmter Sicherheitsstandards bedeutet, welche die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen. Hierzu gehören Sicherheitsvorkehrungen in oder bei der Anwendung von informationstechnischen Systemen oder Komponenten. Es ist bereits heute absehbar, dass der Gesetzgeber wohl schon in naher Zukunft die Etablierung gewisser IT-Standards als eine gesetzliche Verpflichtung ausgestalten wird. Erforderlich hierfür ist jedoch, dass ein Konsens bezüglich allgemein gültiger Standards für IT-Sicherheit gefunden werden kann.

Zu den wichtigsten Eckpfeilern der IT-Sicherheit gehört es, im Unternehmen einen entsprechenden Prozess „IT-Sicherheitsmanagement“ zu etablieren und kontinuierlich zu betreiben sowie eine funktionierende Sicherheitsorganisation zu schaffen. Zu den Aufgaben für den CIO bzw. den IT-Sicherheitsverantwortliche gehört es dabei auch, den Überblick über die abzusichernden Geschäftsprozesse zu bewahren und angemessene Sicherheitsmaßnahmen umzusetzen. Beispielsweise bietet der IT-Grundschutz des BSI eine einfache Methode, die dem Stand der Technik entsprechende IT-Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Mit der Kombination aus der IT-Grundschutz-Vorgehensweise[11] und den IT-Grundschutz-Katalogen stellt das BSI für die Sicherstellung von IT-Security sowohl eine Sammlung von IT-Sicherheitsmaßnahmen als auch eine entsprechende Methodik zur Auswahl und Anpassung geeigneter Maßnahmen zur Verfügung. Zudem werden die IT-Grundschutz-Kataloge des BSI ständig aktualisiert.

Um für die Geschäftsleitung und eine spätere Prüfung darzulegen, dass ein funktionsfähiges Informationssicherheits-Managementsystem etabliert und angemessene Sicherheitsmaßnahmen umgesetzt wurden, kann es unter Umständen sinnvoll sein, eine formale Zertifizierung anzustreben. Die erste internationale Norm für eine solche Zertifizierung des IT-Sicherheits-Management ist ISO 27001. Das BSI hat die Zertifizierung dieser abstrakten Vorgaben um die konkreten IT-Grundschutz-Empfehlungen erweitert. Eine derartige ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz umfasst sowohl eine Prüfung des IT-Sicherheitsmanagements als auch der konkreten IT-Sicherheitsmaßnahmen auf Basis von IT-Grundschutz.

Die in einem Unternehmen notwendigen Maßnahmen für eine so verstandene „Information Security Governance“ sollten sich trotz der Möglichkeit einer solchen Zertifizierung stets an den individuellen Bedürfnissen des Unternehmens (und nicht der jeweiligen Softwareanwendungen) orientieren. Die IT-Architektur sollte demgemäß im Idealfall eine wirklich „Service Orientated Architecture“ (SOA) aufweisen.[12]

Erste Maßnahmen im Bereich IT-Security beginnen mit so scheinbar trivialen Aspekten wie der Festlegung von Verantwortlichkeiten und Befugnissen der IT-User. Nur durch ein sorgfältig ausgearbeitetes Konzept für die Vergabe von Lese- und Editierrechten lässt sich erreichen,

---

11 Die IT-Grundschutz-Vorgehensweise beschreibt Schritt für Schritt, wie ein IT-Sicherheitsmanagement in der Praxis aufgebaut und betrieben werden kann. IT-Grundschutz interpretiert so die eher allgemein gehaltenen Anforderungen der ISO-Standards 13335, 17799 und 27001.

12 Siehe zu SOA bei Ultra-Large-Scale-Systemem, N.N., Computerwoche 10/2007, 38 f.

dass die jeweiligen betriebswesentlichen Informationen tatsächlich nur von den hierzu berechtigten Mitarbeitern gelesen und (über eine Versionskontrolle der in der Datenbank vorhandenen Dokumente) bearbeitet werden können. Zudem kann durch die Steuerung der Zugriffsberechtigungen die auch aus dem Blickwinkel des Risikomanagements erforderliche Funktionstrennung (sog. „Segregation of Duties, SOD") gewährleistet werden. Diese SOD sollte allerdings system- und plattformübergreifend ausgestaltet sein, weil sonst die eingerichteten Sicherheitsprozesse zu leicht umgangen werden können. Bei der Ausarbeitung solcher interner Security-Policies können ebenfalls spezielle IT-Standards helfen. Neben internen Sicherheitsrichtlinien ist selbstverständlich ein weiterer unerlässlicher Bestandteil von IT-Security der Schutz der Systeme gegen Angriff von außen, insbesondere durch den Einsatz von systemadäquaten und aktuellen Firewalls, Virenschutz- und Anti-Spam-Software.

Bei der Einschaltung externer IT-Dienstleister ist es zudem erforderlich, für die vorhandenen IT-Systeme entsprechende Wartungs- und Pflegeverträge sowie Service Level Agreements (SLA) abzuschließen. Je nach Bedeutung der IT-Systeme müssen diese dann optimalerweise redundant, zumindest aber in dezidierten Serverräumen mit Zugangskontrollen und ggf. mit unterbrechungsfreier Stromversorgung vorgehalten werden, um Schäden bei einem Ausfall der betriebsnotwendigen IT-Systeme vorzubeugen. Zudem muss das Management sich bereits im Vorfeld von denkbaren Notfällen Gedanken über Backup- und Recovery-Strategien gemacht haben.

3.5 Datenschutz und Datensicherheit

IT-Compliance bedeutet auch die Einhaltung und Sicherstellung von Datenschutz und Datensicherheit.

Datenschutz im Sinne von Datensicherheit beinhaltet (auch im Sinne der zuvor beschriebenen IT-Security) zunächst die Etablierung von technischen und organisatorischen Maßnahmen, die erforderlich sind, um den Schutz von (teilweise auch personenbezogenen) Daten sicherzustellen. Die Anlage zu § 9 BDSG enthält hierzu konkrete Schutzziele, die vom Unternehmer zum Schutz der im Unternehmen vorhandenen Daten zu ergreifen sind. Es handelt sich um die sog. „8 goldenen Regeln des Datenschutzes", die in der Anlage zu § 9 Satz 1 BDSG explizit aufgeführt sind:

- **Zutrittskontrolle**
  Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, müssen im Wege der Zutrittskontrolle vor unbefugtem Zutritt geschützt werden, sich also beispielsweise in besonders gesicherten Räumlichkeiten befinden.
- **Zugangskontrolle**
  Der Zugang zum EDV-System muss geschützt sein, etwa durch Passwörter, welche nicht schnell geknackt werden können.

- **Zugriffskontrolle**
  Auch der Zugriff auf die personenbezogenen Daten muss anhand der Vergabe von Zugriffsrechten kontrolliert werden.

- **Weitergabekontrolle**
  Mit der Weitergabekontrolle soll verhindert werden, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes unbefugt gelesen, kopiert, verändert oder entfernt werden können. Zudem soll überprüft werden können, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen der Datenübertragung vorgesehen ist. Die Weitergabekontrolle betrifft deswegen insbesondere Daten, die über Netzwerke fließen. E-Mails, die personenbezogene Daten enthalten, sind im Rahmen der Weitergabekontrolle grds. besonders (bspw. durch Verschlüsselung) zu schützen.

- **Verfügbarkeitskontrolle**
  Personenbezogene Daten müssen gemäß den Vorgaben des Datenschutzrechtes ständig verfügbar sein und insbesondere vor zufälliger Zerstörung geschützt werden.

- **Trennungsgebot**
  Daten, die zu verschiedenen Zwecken erhoben wurden, müssen getrennt voneinander verarbeitet werden. Dabei verlangt der Gesetzgeber keine physikalische Trennung der Daten; auch eine logische Trennung ist grds. ausreichend.

- **Eingabekontrolle**
  Eine revisionssichere Protokollierung der Eingaben ist nicht nur nach GOBS, sondern auch nach dem BDSG erforderlich.

- **Auftragskontrolle**
  Die durch einen Dritten im Auftrag verarbeiteten Daten des Auftraggebers dürfen nur im Rahmen der Weisungen des Auftragsgebers verarbeitet werden.

Neben diesen eher organisatorischen Anforderungen an Datensicherheit bedeutet IT-Compliance auch die Einhaltung von „materiellem“ Datenschutzrecht, also die Befolgung der Vorgaben für die Erhebung, Speicherung und Nutzung von personenbezogenen Daten im Unternehmen. Gerade bei der privaten Nutzung von Internet und E-Mail im Unternehmen spielen daher das BDSG, das TMG und das TKG eine wesentliche Rolle.[13]

Das BDSG stellt zudem verschiedene formelle Vorgaben auf, die es im Rahmen von IT-Compliance ebenfalls zu beachten gilt. Dazu gehören unter bestimmten Voraussetzungen die Bestellung eines Datenschutzbeauftragten, die Erstellung und Bereithaltung einer Verfahrensübersicht, die Durchführung von Vorabkontrollen und die Schulung der Mitarbeiter, die mit personenbezogenen Daten umgehen:

So haben öffentliche und nicht öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, einen Beauftragten für den Datenschutz zu bestellen (§ 4 f BDSG), wenn mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten

---

13 Vgl. dazu *Rath/Karner*, K&R 2007, 446-452.

beschäftigt sind. Der Datenschutzbeauftragte hat zudem die Aufgabe, auf die Einhaltung des BDSG und anderer Vorschriften des Datenschutzes hinzuwirken. Verantwortlich für die Einhaltung der Vorschriften bleibt aber trotz der Bestellung eines Datenschutzbeauftragten die Unternehmensleitung; der Datenschutzbeauftragte ist lediglich ein Kontrollorgan. Der Datenschutzbeauftragte ist der Unternehmensleitung direkt unterstellt, ist aber in seiner Tätigkeit weisungsfrei. Aus der Kontrollfunktion des Datenschutzbeauftragten folgt, dass bestimmte Personen nicht zum Datenschutzbeauftragten bestellt werden dürfen, so z. B. der Inhaber eines Unternehmens, der Vorstand, der Geschäftsführer oder ein sonstigen Leiter eines Unternehmens. Bei allen anderen Personen muss geprüft werden, ob ein Interessenkonflikt gegeben sein könnte. Nach allgemeiner Auffassung ist ein solcher Interessenkonflikt z. B. beim CIO, also dem Leiter der EDV, gegeben.

Aus Sicht der IT-Compliance ist zu bemängeln, dass insbesondere die Verpflichtung zur Erstellung einer Verfahrensübersicht oftmals nicht beachtet wird. Diese hat ihre gesetzliche Grundlage in § 4 g Abs. 2 Satz 1 BDSG: „Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4 e Satz 1 BDSG genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen.“ Dabei ist nicht etwa der Datenschutzbeauftragte für die Erstellung und Aktualisierung der Verfahrensübersicht verantwortlich, sondern die für den Datenschutz verantwortliche Stelle, also das Unternehmen.

Unter bestimmten Voraussetzungen ist das Unternehmen zudem verpflichtet Vorabkontrollen durchzuführen. Dies ist dann der Fall, wenn automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Als besonders risikoreich gelten vor allem die Verarbeitung besonderer Arten personenbezogener Daten.

3.6 Elektronische Speicherung von Dokumenten

Es ist bereits angeklungen, dass IT-Compliance auch bei der elektronischen Archivierung von Dokumenten relevant wird. Kaufleute müssen nach Handelsrecht (§ 257 HGB), aber auch aus steuerrechtlichen Gründen (§ 147 AO) die von ihnen empfangenen und abgesendeten Handels- und Geschäftsbriefe aufbewahren.[14] Dennoch sollte der Unternehmer im eigenen Interesse bei der Einführung entsprechender Prozesse zwischen steuerrelevanten Daten und (lediglich) archivierungspflichtigen Informationen unterscheiden.

Die Aufbewahrungsfrist für Handelsbriefe beträgt nach § 257 Abs. 4 HGB (ebenso wie nach § 147 Abs. 3, 4 AO) sechs, für Buchungsbelege, Jahresabschlüsse, etc. bis zu zehn Jahre. Da der Rechtsverkehr im Unternehmen heutzutage größtenteils elektronisch erfolgt, sind neben den vorgenannten Dokumenten selbstverständlich auch E-Mails im Zusammenhang mit der Vorbereitung, dem Abschluss und der Durchführung des „Handelsgeschäftes“ i.S.v.

---

[14] Siehe zur Aufbewahrungspflicht von E-Mails *Böhme*, K&R 2006, 176 ff.

§ 343 HGB zu archivieren.[15] Nach §§ 239 Abs. 4, 257 Abs. 3 HGB können solche „Geschäftsbriefe“ auch auf Datenträgern aufbewahrt werden, wenn dies den Grundsätzen ordnungsgemäßer Buchführung (GoB) und den Grundsätzen ordnungsgemäßer DV-gestützer Buchführungssysteme (GoBS) entspricht. Dann muss allerdings u.a. sichergestellt sein, dass die Daten mit den Originalen übereinstimmen, dass diese innerhalb der Aufbewahrungsfrist verfügbar sind und in angemessener Frist lesbar und maschinell auswertbar gemacht werden können (sog. Revisionssicherheit). Die maschinelle Auswertbarkeit kann ggfls. auch über eine direkte Verlinkung der Dokumente in das (produktive) Buchführungssystem erreicht werden, solange die Unveränderbarkeit gewährleistet ist.

Die ordnungsgemäße Archivierung gemäß dieser Vorgaben wird in der Praxis dadurch erschwert, dass manche E-Mail-Programme bei der Archivierung aus Speicherplatzgründen die Anlagen zu den E-Mails einfach „abschneiden“; das spart Speicherplatz, führt aber spätestens bei der Betriebsprüfung zu einer Beanstandung. Dies gilt zumindest dann, wenn sich unter diesen E-Mails steuerrechtlich relevante Daten befinden. Denn in diesem Fall müssen (zumindest nach Ansicht der Finanzverwaltung) die Inhalte der E-Mails im Originalformat archiviert werden.

Ein weiteres Problem kann auch die immer häufiger anzutreffende Verschlüsselung von E-Mails (Encryption) mit sich bringen. Auch bei der Speicherung von verschlüsselten E-Mails muss während der gesetzlich vorgeschriebenen Aufbewahrungszeit eine Entschlüsselung jederzeit möglich sein. IT-Compliance bedeutet daher auch, dass das Unternehmen eine interne Regelung für die Ablage und Archivierung von E-Mails (E-Mail-Management) vorsehen sollte.[16] Zudem sollte mit Blick auf die bereits angesprochenen ECM-Systeme und die Verfügbarkeit von unternehmensrelevanten Informationen eine Software vorhanden sein, mit der auch unstrukturiert vorliegende, geschäftsrelevante Informationen innerhalb einer angemessenen Zeit einem Projekt zugeordnet werden können. Dies gilt jedenfalls solange, bis E-Mails sog. Metadaten enthalten, die bspw. mit Hilfe der „Extensible Access Method (XAM)“ oder einer anderen Methode eine strukturierte Auswertung der E-Mails erlauben.[17]

Problematisch ist zudem, dass der Lebenszyklus von Softwareanwendungen (und damit auch die Rückwärts-Kompatibilität der Software) immer kürzer wird und auch die Anforderungen an die IT-Systeme sich kontinuierlich ändern. Auch wenn sich die Etablierung eines speziellen „(Information)-Lifecycle-Management“-Systems wohl nur in großen Konzernen empfehlen wird, bleibt es bei den zuvor skizzierten Aufbewahrungsfristen. Hinzu kommt, dass auch das neue DV-System die Unveränderbarkeit des Datenbestandes gewährleisten muss (§ 146 Abs. 4 AO). Im Falle eines Releasewechsels, eines Austauschs der Produktiv- oder E-Mail-Systeme oder gar eines vollständigen Wechsel des IT-Providers müssen daher die (unveränderten) Altdaten revisionssicher in das neue IT-System übertragen oder aber während

15 Im Hinblick auf die Archivierung von steuerrechtlich relevanten Daten kann es sich empfehlen, im E-Mail-Programm eine Schnittstelle zu integrieren, die bei Aktivierung zu einer Buchungsanweisung führt.

16 Vgl. auch *Hauschka*, ZRP 2006, 258, 259.

17 Vgl. hierzu die Initiative der Storage Networking Industry Association (SNIA), Computerwoche 17/2007, 17.

der Aufbewahrungspflicht in zwei Systemen parallel verfügbar gehalten werden. Neben Authentizität und Integrität der Dokumente muss im Langzeitarchiv auch noch die Lesbarkeit garantiert werden. Dies führt in der Praxis oft zu einer kostenträchtigen redundanten Datenhaltung.[18] Problematisch ist hier zudem, dass die Rückwärtskompatibilität von Softwareprogrammen und Formaten zeitlich begrenzt ist.

3.7 Elektronische Prüfung / GDPdU

Um Dritten (insbesondere dem Betriebsprüfer) eine Prüfung der häufig unmittelbar aus den ERP-Systemen (Enterprise Ressource Planning) und Buchhaltungssystemen generierten Informationen zu ermöglichen, muss die Archivierung idealerweise von Anfang an so erfolgen, dass die Dokumente periodengerecht den jeweiligen (Handels-) Geschäften zugeordnet werden können. Hierzu kann es ggfls. auch notwendig sein, dass auch die Anlagen zu einer E-Mail aufbewahrt werden, da der in einer E-Mail verkörperte Handelsbrief ohne die zugehörigen Attachments regelmäßig nicht verständlich oder zur Dokumentation des Geschäftsvorfalles unzureichend wäre.[19] Die Herausforderung liegt darin, dass integrierte ERP-Systeme heutzutage völlig neue Prozesslogiken aufweisen und die originäre Erfassung rechnungslegungsrelevanter Daten in operative Bereiche außerhalb der Buchführung verlagern. Dennoch gelten auch für diese Systeme die allgemeinen Anforderungen an die Archivierung digitaler Unterlagen nach § 147 AO (insbesondere die GoBS), die vom Bundesfinanzministerium (BMF) durch die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)“ aus dem Jahr 2001 konkretisiert wurden. Der Finanzverwaltung steht danach bereits seit dem 1. Januar 2002 bei Außenprüfungen das Recht zu, nach Maßgabe der GDPdU auf alle digitalen steuerrelevanten Unternehmensdaten zuzugreifen. Danach sind die Unternehmen auf Anfrage des Steuerprüfers dazu verpflichtet, ihre steuerrelevanten Daten (also zumindest die Finanz-, Anlagen und Lohnbuchhaltung, wohl aber auch die ECM-Systeme) maschinell auswertbar zur Verfügung zu stellen.

Praxishinweis

> Bei der Außenprüfung werden drei Arten des Datenzugriffs unterschieden: der unmittelbare Lesezugriff durch Verwendung der unternehmenseigenen Hard- und Software (Z1), der mittelbare Zugriff über Auswertungen des Unternehmens nach den Vorgaben des Prüfers (Z2) und die (ggfls. nach dem Standard des BSI zusätzlich verschlüsselte) Datenüberlassung (Z3), wobei es für letztgenannten Datenzugriff durch den Betriebsprüfer ebenfalls

[18] Siehe zu den Anforderungen an sog. „auswertbare Archive“ auch Projekte wie Archisig [www.archisig.de] und das Nachfolgeprojekt Transidoc [www.transidoc.de].

[19] Allerdings warden E-Mails nicht in den GDPdU, sondern nur in den Q&A der Finanzverwaltung erwähnt. Für den Datenzugriff sind E-Mails wegen der fehlenden Datenstruktur zudem nur eingeschränkt geeignet.

> Empfehlungen des Bundesfinanzministeriums gibt. Die Daten werden dann in der Regel in die Prüfsoftware „IDEA“ oder „ACL“ eingelesen. Unterstützt wird der Datenzugriff durch Makros, welche die Auswertung der beim Unternehmen vorhandenen Informationen erleichtern.[20] Ein Online-Zugriff auf die Datenbestände des Unternehmens ist der Finanzverwaltung jedoch (derzeit) nicht gestattet.

Das BMF hat die „Fragen und Antworten zum Datenzugriff der Finanzverwaltung“ wiederholt aktualisiert und gibt nunmehr noch mehr Antworten zu dem digitalen Datenzugriff, etwa bezüglich des Zugriffs des Prüfers auf das Intranet des Unternehmens. Trotz dieser Klärung einzelner Streitpunkte bleibt vor allem die Frage der Einordnung der im Unternehmen vorhandenen Daten als „steuerrelevant“ von entscheidender Bedeutung. Für eine solche steuerrechtliche Relevanz ist grundsätzlich keine steuerliche Auswirkung erforderlich; aus diesem Grund können ggfls. auch freiwillig erstellte, digitale Aufzeichnungen (insbesondere für DMS-Systeme neu eingescannte Dokumente) oder gar Informationen zu Kostenstellen dem Datenzugriff der Finanzbehörden unterliegen. Aus dem Fragen- und Antwortenkatalog geht beispielsweise hervor, dass die steuerliche Außenprüfung nunmehr auch auf den Zugriff auf ECM-Systeme ausgedehnt wird. Daraus folgt, dass auch eingescannte Dokumente als originär digitale Unterlagen anzusehen sind, mit der Folge, dass auch für ein ECM-System die in den GDPdU beschriebenen Zugriffsarten gelten. Diese Interpretation wurde auch im Urteil des 2. Finanzgerichtes Düsseldorf vom 5. Februar 2007 bestätigt.[21] Hinzu kommt, dass nach Meinung der Finanzverwaltung elektronische Post im Originalformat (E-Mail-Format) archiviert werden muss. Firmen kommen damit nicht umhin, neben Langzeitformaten wie TIFF und PDF/A[22] auch das (proprietäre) Originalformat zu archivieren.[23] Zudem ist die Frage, welche Dateiformate archivtauglich sind, noch nicht abschließend geklärt. In zahlreichen Unternehmen gilt seit Jahren das Format „TIFF-G4“[24] als Defacto-Standard, für farbige Vorlagen ist das Bildformat JPEG gebräuchlich.[25] Diese Formate bieten neben der (derzeitigen) Revisionssicherheit auch Möglichkeiten für die Auswertung strukturierter Inhalte, was eine Vollindizierung ermöglicht. Allerdings gibt es keine entsprechende ISO-Norm für eine gesetzeskonforme Archivierung mit diesen Formaten.

Auch in diesem Zusammenhang wird die Bedeutung des zuvor skizzierten User-Management nochmals deutlich: dem Betriebsprüfer sollen schließlich nur diejenigen Teile der Dokumentationssammlung zur Verfügung gestellt werden, welche den Prüfungsbereich und die richtige

---

[20] Bspw. AIS TaxAudit 2007 R 1 (Audit Information System der Fa. Audicon GmbH).

[21] Die Richter hatten sich mit der Frage zu befassen, inwieweit Eingangsrechnungen, welche mit Hilfe einer softwaregestützten Belegarchivierung eingescannt und anschließend im Original vernichtet wurden, dem Recht auf Datenzugriff unterliegen, obwohl es sich möglicherweise nicht um originär digitale Daten im Sinne der GDPdU handelt. Das FG Düsseldorf urteilte, dass auch diese Belege „mit Hilfe einer Datenverarbeitungsanlage erstellt“ wurden und damit dem Zugriffsrecht der Finanzbehörden unterlägen.

[22] Zertifiziert nach ISO 19005-1:2005.

[23] Vgl. auch *Brand*, Computerwoche 39/2007, 16-17.

[24] TIFF-G4-Dateien sind monochrome S/W-TIFFS.

[25] Seit kurzem neu hinzugekommen sind der PDF/A-Standard und XPS (die Abkürzung steht für „XML Paper Specification“, entwickelt von Microsoft und seit Ende 2006 mit Vista verfügbar).

Prüfungsperiode betreffen. Das EDV-System muss daher (zumindest im Interesse des Unternehmens) zur Vermeidung von erheblichen Zusatzkosten von vornherein eine Trennung der steuerlich relevanten Daten von den übrigen archivierungspflichtigen Daten sowie eine Differenzierbarkeit nach Jahren und Steuerarten ermöglichen.

3.8 Electronic Invoicing

Wenn im Unternehmen Rechnungsdaten und Rechnungen ohnehin elektronisch generiert und archiviert werden, liegt es nahe, diese auch elektronisch zu unterzeichnen. Die elektronische Rechnung und das Signieren elektronischer Dokumente mit einer qualifizierten digitalen Signatur nach dem Signaturgesetz (SiG) führen aufgrund deren Komplexität bislang ein Schattendasein. Zudem ist es für die weitere Verbreitung des Electronic Invoicing sicherlich auch nicht förderlich, dass – trotz des Harmonisierungsbefehls des EU-Gesetzgebers – die Vorgaben bezüglich der Anerkennung elektronischer Rechungen europaweit nicht ganz einheitlich sind. Gerade in großen Unternehmen und Konzernen kann aber der (auch grenzüberschreitend) mögliche Einsatz von Electronic Invoicing als weiterer Bestandteil von IT-Compliance erhebliche Einsparpotenziale mit sich bringen.

3.9 Rechtskonforme IT-Systeme / Lizenzmanagement

Der Begriff IT-Compliance beschreibt darüber hinaus die Anforderungen, welche an die im Unternehmen vorhandenen IT-Systeme zu stellen sind. Im Ergebnis bedeutet dies, dass auch die dort vorhandenen IT-Systeme (Hardware und Software) selbst rechtskonform sein müssen. Die diesbezüglichen Anforderungen sind vielfältig und sollen daher nachfolgend ebenfalls nur umrissen werden.

Rechtskonforme IT-Systeme sind beispielsweise nur solche, die ihrerseits über ausreichende „Lizenzen“ (also Nutzungsrechte) zum Betrieb der jeweiligen Software verfügen – einen gutgläubigen Erwerb von Rechten an einer Software gibt es nicht. Die Unternehmensleistung muss daher (ggfls. durch ein Software Asset Management) sicherstellen, dass die zum Betrieb der im Unternehmen vorhandenen Software erforderlichen Nutzungsrechte vorhanden sind. Dies ist allerdings oftmals vollkommen uneingeschränkt nur bei dem erstmaligen Erwerb der jeweiligen Software der Fall. Zumindest nach einer Expansion, einer Fusion mit einem anderen Unternehmen oder einer Auslagerung von Betriebsteilen kann sich diese lizenzrechtliche Situation schnell anders darstellen. Denn der Erwerb einer „Unternehmenslizenz“ bedeutet nicht, dass es keine weiteren Nutzungsbeschränkungen für die Software gibt. Das Gegenteil ist häufig der Fall: oftmals gibt es (dingliche) Beschränkungen des zulässigen Nutzungsum-

fangs, etwa durch eine maximale Anzahl von „named user“, „concurrent user“ oder sonstigen Nutzungs- und Weitergabeverboten. Diese Einschränkungen gelten grundsätzlich auch beim Erwerb „gebrauchter Software“. Durch die Etablierung eines Softwarelizenz-Managementsystems kann aber nicht nur eine (auch strafrechtlich relevante) Unterlizenzierung vermieden werden. Vielmehr kann oft auch eine kostenträchtige Überlizenzierung und so Kosteneinsparpotenziale identifiziert werden.[26]

4. IT-Compliance mit und durch IT-Standards

IT-Compliance insgesamt, aber vor allem IT-Security, ist ohne die Einrichtung und Beachtung branchenüblicher und anerkannter IT-Standards nicht möglich. Wie schon zuvor gezeigt, geht auch § 2 Abs. 2 BSIG davon aus, dass Sicherheit in der Informationstechnik die Einhaltung bestimmter (Sicherheits-) Standards bedeutet. Zudem füllen IT-Standards unbestimmte Rechtsbegriffe aus und legen Methoden zur Ermittlung und Sicherstellung des aktuellen Standes der Technik für IT-Leistungen fest. Dies bedeutet nicht, dass die Einhaltung von IT-Standards derzeit gesetzlich gefordert ist; im Falle des Schadenseintrittes wird jedoch die Frage gestellt werden, warum man sich nicht um die Einhaltung anerkannter Standards bemüht hat.

4.1 Die Suche nach dem passenden IT-Standard

Bei der Suche nach den für das jeweilige Unternehmen „richtigen“ IT-Standards hat die Geschäftsleitung die Qual der Wahl. Zudem wird die Lesebegeisterung des IT-Anwenders auf eine harte Probe gestellt:

So umfassen bspw. die allgemein anerkannten Standards für IT-Sicherheit des BSI und die zuvor bereits beschriebenen IT-Grundschutz-Kataloge, nebst den zugehörigen BSI-Standards (vormals IT-Grundschutzhandbuch [GSHB] genannt) weit über 3.000 Seiten. Diese (im Bundesanzeiger-Verlag als Printversion erhältlichen) Grundschutz-Kataloge zeigen allerdings sehr anschaulich verschiedene Gefährdungslagen auf und geben Empfehlungen zur Risikominderung; das ebenfalls vom BSI angebotene „GS Tool“ hilft bei der Erfassung und Auswertung.

[26] Laut einer Untersuchung von *Gartner* geben Unternehmen ohne ein effizientes Lizenzmanagementsystem bis zu 60% zu viel für Software aus.

Neben diesem weit verbreiteten IT-Security-Standard des BSI gibt es beispielsweise die so genannten „Control Objectives IT (CobiT)“ und den zwischenzeitlich als Quasi-Standard für methodenorientierte IT-Abteilungen anerkannten ITIL-Katalog, also die aus dem angelsächsischen Behördenumfeld stammenden „Best Practices“-Sammlung „ITIL (IT Infrastructure Library)“.

Derzeit gibt es allerdings keinen übergreifenden, national oder international verbindlichen Standard für die große Palette unterschiedlicher IT-Leistungen. Die Frage, welche Standards für das jeweilige Unternehmen und die betreffende Anwendung richtig sind, kann daher nicht pauschal beantwortet werden. Bei der Auswahl des richtigen Standards kommt es vielmehr auch auf die im Unternehmen und bei dem IT-Dienstleister bereits vorhandenen Prozesse und die Aktualität der einschlägigen Standards an.[27]

Dennoch ist der Trend zur Standardisierung eindeutig. So schreitet beispielsweise auch die Normung von Datenstrukturen insbesondere bei den Finanzinformationen weltweit voran. Dies zeigt sich schon daran, dass US-Börsenaufsicht, Europäische Bankenaufsicht und der Elektronischer Bundesanzeiger beim neuen Elektronischen Handelsregister für den Informationsaustausch von Finanzinformationen auf den Standard „XBRL (eXtensible Business Reporting Language)“ setzen.[28] Auch für die Archivierung von elektronischen Daten gibt es inzwischen einen international anerkannten Standard, die ISO 15489.

4.2 Die Rechtsfolge der Einhaltung von IT-Standards

In rechtlicher Hinsicht ist es für die Geschäftsleitung des Unternehmens im Zweifel etwas unbefriedigend, dass die Vorgaben für IT-Compliance entweder in einer ganzen Reihe von Normen „versteckt“ oder aber so wenig konkret sind, dass selbst bei deren gewissenhafter Umsetzung noch immer Zweifel bestehen können, ob alle Vorgaben eingehalten sind. Auch die zuvor genannten, vermeintlich speziellen IT-Regelwerke enthalten nur wenige eindeutige Vorgaben zur Sicherstellung von IT-Compliance. Zudem entfalten diese Werke und IT-Standards – zumindest bislang – weder unmittelbare Rechtswirkung noch resultiert aus deren Anwendung eine (unwiderlegliche) Vermutung für die Rechtskonformität und damit die Einhaltung von IT-Compliance.

Weiterhin ist problematisch, dass es nur wenige wirklich konkrete Vorgaben an die IT gibt, welche überhaupt normativen Charakter haben, geschweige denn formalen Gesetzesrang einnehmen. Hierzu zählen beispielsweise beim IT-Outsourcing die bankenspezifischen Vorgaben der §§ 25 a KWG, 33 Abs. 2 WpHG, die für Banken und Finanzdienstleister durch spezifische Rundschreiben ergänzt werden (beispielsweise bezüglich des Outsourcing gemäß

---

[27] Siehe hierzu auch die nachstehend abgebildete Tabelle zu den IT-Standards.

[28] Weitere Informationen zu dem neuen Standard für Jahresabschlüsse und sonstige Finanzinformationen unter www.xbrl.de.

§ 25 KWG das RS 11/2001 des BAKred, heute BaFin) und das RS 18/2005 des BaFin, mit dem Mindestanforderungen für das Risikomanagement (MaRisk) aufgestellt werden. In den MaRisk hat die BaFin zur Konkretisierung der Vorgaben des § 25 a Abs. 1 KWG die zuvor aufgestellten Mindestanforderungen an das Betreiben von Handelsgeschäften (MAH), die Mindestanforderungen an die Ausgestaltung der internen Revision (MaIR) und die Mindestanforderungen an das Kreditgeschäft (MaK) der Kreditinstitute konsolidiert und ergänzt. In den neuen Rahmenvorgaben werden Pflichten bezüglich der Ausgestaltung der Leitungs-, Steuerungs- und Kontrollprozesse als Bestandteile des internen Risikomanagement festgelegt. So wird u.a. die Einhaltung der BSI-Standards für den IT-Grundschutz verlangt.[29]

Mit den MaRisk werden die Mindestanforderungen definiert, die Finanzinstitute bei ihrem Risikomanagement umzusetzen haben. In den MaRisk wird zudem hervorgehoben, dass die operationellen Risiken inklusive der IT-Risiken integraler Bestandteil des Risikomanagements sind. Hierdurch ergeben sich auch Forderungen an die IT-Sicherheit von Banken. Explizit mit IT-Sicherheit beschäftigt sich Abschnitt AT 7.2 („Technisch-organisatorische Ausstattung") der MaRisk: Danach haben sich Umfang und Qualität der technisch-organisatorischen Ausstattung insbesondere an betriebsinternen Erfordernissen, den Geschäftsaktivitäten, der Risikostrategie sowie der Risikosituation zu orientieren. Die IT-Systeme und die zugehörigen IT-Prozesse müssen daher die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen. Für diese Zwecke ist bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen. Die Wahl der Standards ist zu begründen. Ihre Eignung ist regelmäßig von den fachlich und technisch zuständigen Stellen zu überprüfen. Neue IT-Systeme sowie Veränderungen an IT-Systemen sind vor ihrem Einsatz zu testen und von den fachlich und technisch zuständigen Stellen abzunehmen. Produktions- und Testumgebung sind dabei grundsätzlich voneinander zu trennen. Die Entwicklung und Änderung programmtechnischer Vorgaben (z. B. Bewertungsalgorithmen) haben unter Beteiligung aller fachlich und technisch zuständigen Stellen zu erfolgen. Die programmtechnische Umsetzung hat grundsätzlich durch eine vom Anwender unabhängige Stelle zu erfolgen. Weiterhin gibt es noch ergänzende Erläuterungen im Dokument „MaRisk – Regelungstext mit Erläuterungen". Hier wird ebenfalls auf die Auswahl von Standards zum IT-Sicherheitsmanagement eingegangen und auf die BSI-Standards verwiesen.

Die zunächst nur für Kreditinstitute einschlägigen Anforderungen der MaRisk (man beachte die Neufassung des § 25 a KWG ab 1. November 2007) können mit ihren unterschiedlichen Modulen als „Best Practice" auch in Unternehmen zur Anwendung kommen, die nicht zum Banken- und Finanzdienstleistungs-Sektor gehören. Denn auch interne Richtlinien und Verwaltungsvorschriften von eigentlich für das Unternehmen gar nicht zuständigen Behörden (wie etwa die IT-Richtlinie des BMI hinsichtlich des Einsatzes von IT-Systemen in den obersten Bundesbehörden) können wertvolle Ansatzpunkte für die Umsetzung von IT-Compliance im Unternehmen enthalten.

---

29 Siehe AT 4.3.2 MaRisk; Modul BTR 4.

5. Das Damokles-Schwert der Haftung

Etwaige Nachlässigkeiten im Bereich IT-Compliance werden nicht nur bei einer steuerlichen Betriebsprüfung oder im Falle einer M&A-Transaktion (und der dieser vorangehenden Due Diligence) bestraft. Vielmehr sind die Grenzen unternehmerischer Handlungsfreiheit dann erreicht, wenn ein Vorstandsmitglied gegen die vorstehend nur skizzierten, aber im Wesentlichen anerkannten Erfahrungsgrundsätze verstößt. So wurde bspw. vom LG München[30] der Hauptversammlungsbeschluss zur Entlastung des Vorstandes für nichtig erklärt, weil es bei einem Münchner Großhändler für Mikroelektronik u.a. an der schriftlichen Dokumentation des Risikomanagements und der dahinter liegenden IT-Struktur fehlte.

Die Palette der denkbaren Sanktionen bei Verstößen gegen IT-Compliance-Anforderungen reicht – je nach Zielrichtung der verletzten Norm – neben den zuvor beschriebenen Folgen von drakonischen Maßnahmen wie Haft, Verhängung von Geldbußen, Hausdurchsuchungen und Bußgeldverfahren wegen Aufsichtspflichtverletzung gegen geschäftsführende Organmitglieder über zivilrechtliche Ansprüche gegen Organe der Gesellschaft (§§ 91, 93, 116 AktG) bis hin zur Abschöpfung des „gesamten wirtschaftlichen Wertes“ durch Verfall (§§ 73 StGB, 29 a OWiG) und Schadensersatzansprüchen von Wettbewerbern (etwa § 33 GWB). Daneben kann es zu steuerrechtlich unerwünschten Folgen (Abzugsverbot, Schätzung) wie auch zu negativen Folgen für das Rating des Unternehmens nach Basel II kommen. Bislang sind allerdings – zumindest in Deutschland – außer dem vorgenannten Fall des LG München noch keine Fälle von mangelnder IT-Compliance bekannt geworden, bei denen dieses Sanktionsinstrumentarium mit aller Schärfe zur Anwendung kam.

6. Fazit

Die vorstehend skizzierten IT-spezifischen Branchenkenntnisse sind naturgemäß nicht von jeder Geschäftsleitung zu erwarten. Es stellt jedoch auch kein Allheilmittel dar, sich auf den Sachverstand eines externen IT-Dienstleisters oder des CIO zu verlassen, denn eine vollständige Delegation der zuvor skizzierten Pflichten kann damit ebenso wenig erreicht werden wie mit der internen Aufgabenverlagerung und der Schaffung von Positionen eines CIO oder CSO. Dennoch wird gerade auch bei einer Auslagerung der IT-Systeme auf einen externen IT-Provider oftmals nur auf die Verbesserung der Kostenquote geschielt, anstatt bei dem Fremd-Outsourcing auch auf die notwendige „law compliance“ zu achten.[31]

---

30 LG München v. 5.4.2007 – 5 HKO 15964/06, AG 2007, 417 ff.

31 Vgl. hierzu auch die Bitkom-Studie Compliance in IT-Outsourcing-Projekten (2007), abrufbar unter http://www.bitkom.org/files/documents/BITKOM-Leitfaden_Compliance.pdf.

Trotz der komplexen Kombination aus Recht, Steuern und Technik müssen die im Unternehmen eingesetzten IT-Systeme den hohen Anforderungen von IT-Compliance genügen und dürfen nicht als zu vernachlässigende „Commodity“ angesehen werden. Zu den Pflichten einer vorausschauenden Unternehmensleitung gehört es vielmehr, ein angemessenes Informations- und Risikomanagement zu etablieren und rechtskonforme IT-Systeme einzusetzen. Branchenübliche IT-Standards wie ISO, CobiT, ITIL und die IT-Grundschutz-Kataloge des BSI sind inzwischen allgemein anerkannt und helfen bei der Erfüllung der Anforderungen der IT-Compliance.

IT-Compliance bietet aber neben der Vermeidung einer persönlichen Haftung der Geschäftsleitung auch die Möglichkeit, Kosteneinsparungspotenziale zu identifizieren (etwa bei der Vermeidung eines Parallelbetriebes von IT-Systemen oder von Überlizenzierung) sowie eine gute Chance zum Aufbau wirklich prozessorientierter IT-Systeme (SOA), vor allem bei einer intelligenten Kombination der Erfüllung gesetzlicher Archivierungsanforderungen mit der Schaffung effektiver Dokumentenmanagement-Systeme. Auf dem Markt gibt es bereits eine große Auswahl entsprechender Compliance-Management-Software.[32] Ziel muss es allerdings sein, keine Insellösungen für einzelne Anforderungen zu schaffen, sondern eine IT-Strategie zu finden, die neben der Erfüllung von IT-Compliance-Anforderungen auch für den Geschäftsbetrieb insgesamt nutzbringend ist.

Mindestanforderungen an IT-Compliance sind jedoch in jedem Fall die Erstellung einer schriftlichen Verfahrensdokumentation des jeweiligen Systems, die Aufstellung von Archivierungs- und Unternehmensrichtlinien (z. B. zur E-Mail-Nutzung) unter Berücksichtigung von Datenschutz und IT-Sicherheit sowie die Gewährleistung von Aufbewahrungsfristen und Revisionssicherheit.

7. Annex I: Überblick IT-Standards (Auswahl)

CobiT (Control Objectives IT): Sammlung von Veröffentlichungen und Kontrollzielen („Control Objectives“). COBIT stellt einen allgemein akzeptierten, relativ umfangreichen Standard für IT-Sicherheit und IT-Kontrolle dar (die Management Summary der COBIT ist allerdings auch für Geschäftsführer „lesbar“). pdf-Download auf der Webseite der ISACA, www.isaca.org.

ITIL (IT Infrastructure Library): Sammlung von „Best Practice“-Dokumenten und Informationen zum Aufbau und Betrieb von Dienstleistungen im Rahmen der IT. ITIL beschreibt typische Aufgabenstellungen und systematische Prozessabläufe im Betrieb von IT- Infrastruk-

32 Vgl. statt aller etwa den neuen Geschäftsbereich GRC (Governance Risk Compliance) der SAP AG.

turen und in der Erbringung von IT-Dienstleistungen (IT-Service Management), in deren Mittelpunkt die wirtschaftliche Erfüllung der Unternehmensanforderungen steht. Als umfassende Verfahrens-Bibliothek in diesem Bereich gilt ITIL mittlerweise weltweit als Defacto-Standard und findet in deutschen Unternehmen zunehmend Verbreitung. Während 2005 nur die Hälfte der Unternehmen ITIL im Einsatz hatten, sind es 2007 schon 75 %. Aus juristischer Sicht erscheint ITIL insbesondere interessant in Situationen, in denen der IT- Betrieb vertraglich geregelt werden soll (IT-Outsourcing). Die in sieben Bereiche untergliederten ITIL-Bücher sind unter www.ogc.gov.uk zu beziehen. Der „ITIL-Refresh“ des IT Service Management Forum ist seit Herbst 2007 verfügbar.

ISO/IEC 17799:2000 (neuer Standard: ISO 27001): Das von der ISO (Internationale Organisation für Standardisierung) und der IEC (Internationale Elektrotechnische Kommission) herausgegebene Werk basiert auf dem britischen Standard BS 7799 und stellt eine umfassende Sammlung von Maßnahmen zur Erreichung von Informationssicherheit dar, die allerdings teilweise nur sehr generische Maßnahmen vorschreibt (www.iso.org). Die ISO hat inzwischen nicht nur zusätzlich die Standards ISO 13335 und ISO 17799 überarbeitet, sondern auch die Möglichkeit geschaffen, Informationssicherheitsmanagement-Systeme (ISMS) zu zertifizieren. Für diese Zertifizierung wurde der neue Standard ISO 27001 verabschiedet. Dieser internationale Standard wurde zudem vom BSI durch konkrete Empfehlungen in den IT-Grundschutz-Katalogen erweitert.

BS 7799-1:1999 und BS 7799-2:1999 (British Standard): Sammlung des BSI (British Standards Institute, nicht zu verwechseln mit dem BSI Bundesamt für Sicherheit in der Informationstechnik) von Maßnahmen zur Erreichung von Informationssicherheit (Teil 1) und Anleitung zur Implementierung eines ISMS (Informationssicherheitsmanagementsystems), zu beziehen über die AICPA (www.aicpa.com). Nahezu inhaltsgleich mit ISO/IEC 17799:2000 (jetzt: ISO 27001, s.o.). Vorteil: die Inhalte des Zertifikates ähneln denen des SAS 70-Prozesses (Prüfmethode, mit der Wirtschaftsprüfer die Einhaltung von SOX untersuchen).

BS 15000: War einer der ersten Standards weltweit für das IT Service Management, wird künftig von **ISO 20000** abgelöst werden.

IT-Grundschutz-Kataloge des BSI (Bundesamt für Sicherheit in der Informationstechnik): Sammlung von Empfehlungen für IT-Grundschutz und die Realisierung von IT-Sicherheitskonzepten, wird halbjährlich aktualisiert, ist aufgrund einer englischen Übersetzung inzwischen auch international verbreitet und bietet die Möglichkeit der Zertifizierung. Nähere Informationen: www.bsi.de

CC (Common Criteria for Information Technology Security Evaluation): Nachfolger des Kriterienkataloges der ITSEC und weltweit harmonisierte Zertifizierungsgrundlage, ist auch als ISO-Standard 15408 (www.iso.org) verabschiedet worden.

IFAC International IT Guidelines: Richtlinien des Information Technology Committee der International Federation of Accountants, richtet sich vornehmlich an Wirtschaftsprüfer (IT-Prüfer), trotz englischer Sprachfassung geringe Verbreitung.

EnSEC (Enterprise Security Management): Zertifizierungsstandard der TÜV Secure iT GmbH (TÜV Rheinland Berlin Brandenburg), für Detailmaßnahmen wird auf das IT-Grundschutzhandbuch des BSI referenziert. Die Dokumente wurden vom Deutschen TÜV publiziert (www.tuvdotcom.com).

8. Annex II: IT-Compliance-Checkliste

	IT-Compliance-Bereich / Fragestellung	***compliant***	***non compliant***
		ja	**nein / weiß nicht**
1	**Gibt es für Ihre IT ein Sicherheits- und Notfallkonzept?** – Automatisches Backup / Spiegelung der Server – Masterplan für Systemabsturz und Recovery-Maßnahmen – Redundante Server, USV für bestimmte Server		
2	**Werden die Dokumentationspflichten eingehalten?** – Dokumentation des Risikomanagement – Verfahrensverzeichnis nach BDSG – Schriftliche Dokumentation des ECM / DMS		
3	**E-Mail und Internetnutzung** – Gibt es eine IT-Richtlinie und E-Mail-Policy? Ist die private Nutzung geregelt? – Gibt es eine Regelung bezüglich der Zugriffs-, Editier- und Löschrechte der Nutzer? – Erfolgt eine (Echtzeit-) Archivierung der geschäftlichen E-Mails im Originalformat? – Gibt es Vorgaben bezüglich der Ablage von geschäftlichen E-Mails oder ein (softwaregestütztes) automatisches E-Mail-Management?		

	IT-Compliance-Bereich / Fragestellung	*compliant*	*non compliant*
		ja	**nein / weiß nicht**
4	**Archivierung** – Gibt es ein Archivierungskonzept, dass auch die Einhaltung der Aufbewahrungsfristen sicherstellt? – Ist die Revisionssicherheit / GDPdU-Konformität des Archivierungssystems gewährleistet? – Ist die Archivierung an ein ECM oder DMS gekoppelt?		
5	**Zertifizierung / Standards** – Sind Ihre IT-Systeme oder Teile davon zertifiziert? – Kommen IT-Standards bei Ihnen zum Einsatz? – Gibt es bei Ihnen einen CIO? – Wird ein Lizenzmanagement eingesetzt?		
6	**IT-Security** – Werden personenbezogene und vertrauliche E-Mails sowie USB-Sticks verschlüsselt? – Gibt es eine effektive Spam-Abwehr, einen aktuellen Virenfilter, effektive Firewalls? – Ist der Remote-Access sicher? – Ist Ihr Password länger als 8 Zeichen? – Kann nur der Administrator Software oder Hardware installieren?		
7	**Beauftragung von IT-Dienstleistern** – Sind Ihre externen IT-Dienstleister auf die Einhaltung von IT-Compliance verpflichtet? – Ist der Outsourcing-Vertrag auf aktuellem Stand? – Gibt es pönalisierte SLA?		

	IT-Compliance-Bereich / Fragestellung	***compliant***	***non compliant***
		ja	**nein / weiß nicht**
8	**Datenschutz** – Gibt es einen Datenschutzbeauftragten (nicht der CIO!)? – Werden die „8 Goldenen Regelungen“ eingehalten (Kontrolle Zutritt, Zugang, Zugriff, Weitergabe, Verfügbarkeit, Eingabe, Auftrag und Trennungsgebot)?		
9	**IKS** – Gibt es ein Internes Kontrollsystem (IKS) und IT-gestützte Kontrollen? – Sind diese Prozesse ausreichend dokumentiert?		
10	**Kennen Sie diese Begriffe?** – PDF/A-1a/b, TIFF – GoB, GoBS, GDPdU – WORM – IDW RS FAIT 1-3		

Datenschutzrechtliche Compliance im Unternehmen

Silvia C. Bauer

Zusammenfassung

Im Laufe der letzten Jahre ist das Thema „Datenschutz“ immer mehr in den Fokus der Öffentlichkeit geraten. Nicht nur die Verschärfung der Rechtslage innerhalb Deutschlands bzw. im gesamten europäischen Raum hat dazu beigetragen, sondern auch die stetige Sensibilisierung der Öffentlichkeit hinsichtlich des Umgangs mit ihren Daten. Neben der Forderung nach einer technisch ausgereiften und möglichst sicheren Datenverarbeitung hat sich auch verstärkt ein Bewusstsein gebildet, dass Daten nicht beliebig für jeden Zweck verarbeitet und genutzt werden dürfen. Damit einhergehend sind die Anforderungen an Unternehmen, Daten im Einklang mit den gesetzlichen Vorgaben – also „compliant“ - zu verarbeiten, gestiegen.

Unternehmen müssen die verschiedenen formalen Anforderungen der gesetzlichen Vorgaben wie Meldepflichten, Bestellung von Datenschutzbeauftragten oder Erstellung von Verfahrensverzeichnissen einhalten und daneben sicherstellen, dass auch der Umgang mit den Daten an sich innerhalb des Unternehmens den geltenden Rechtsvorschriften entspricht. Ein Unternehmen sollte daher zielgerichtet den Datenschutz in seine organisatorischen Abläufe integrieren und entsprechende Strukturen etablieren. Thematisch auf den Datenschutz ausgerichtete Schulungen, Verhaltensregelungen und die Benennung von Verantwortlichen sollten daher wesentlicher Bestandteil einer Compliance-Organisation im Unternehmen sein.

1. Einleitung

Informationen sind sicher zu verarbeiten. Ein Unternehmen, das diesen Grundsatz missachtet, setzt sich erheblichen Risiken aus: Verstöße gegen entsprechende nationale oder internationa-

le Vorgaben – insbesondere die Vorgaben des Sarbanes Oxley Acts[1] – können empfindliche Bußgelder oder sogar Freiheitsstrafen nach sich ziehen, ein Sicherheitsleck in der eigenen IT-Infrastruktur oder der Verlust von Daten haben regelmäßig immense wirtschaftliche Auswirkungen, Datenmissbrauch wird häufig durch eine negative Presse abgestraft.

Daher legen Unternehmen immer mehr Wert auf die Sicherheit ihrer IT-Umgebung und den Schutz der von ihnen verarbeiteten Daten. Während in der Vergangenheit häufig die Informationstechnologie und deren Funktionalität als größter Risikofaktor in diesem Zusammenhang galt, setzt langsam ein Umdenken ein: Der Mensch und sein Umgang mit risikobehafteten Vorgängen rückt in den Vordergrund. Das Verantwortungsbewusstsein des Einzelnen bei dem Einsatz und der Nutzung von Informationstechnologie sowie der Verarbeitung von Daten soll geschärft werden. Ziel ist die Identifizierung, Minimierung oder sogar der völlige Ausschluss von datenschutzrechtlichen Risiken. Ein Unternehmen ist dabei maßgeblich auf seine Mitarbeiter angewiesen.

Datenschutzrechtliche Compliance hat deshalb – in enger Verzahnung mit der IT-Compliance – einerseits die Umsetzung von gesetzlich und auch tatsächlich erforderlichen organisatorischen und technischen Maßnahmen durch das Unternehmen zum Ziel; andererseits bezweckt sie die einzelnen Mitarbeiter in die Pflicht zu nehmen und ihnen ihre Verantwortung für einen datenschutzrechtlich korrekten Umgang mit Daten bewusst zu machen. Mitarbeiter sind so zu schulen, dass sie unter Wahrung der Persönlichkeitsrechte des Einzelnen gesetzeskonform Daten verarbeiten und nutzen.

Ziel dieses Abschnitts ist es daher nicht nur einen kurzen Überblick über die vom Unternehmen einzuhaltenden datenschutzrechtlichen Anforderungen zu geben, sondern darüberhinaus zu sensibilisieren, in welchen Bereichen die Mitwirkung der Mitarbeiter essentiell sein kann, um das Unternehmen in die Lage zu versetzen, die in Deutschland geltenden datenschutzrechtlichen Vorgaben umzusetzen und einzuhalten.

Dabei wird zunächst erläutert, wer überhaupt im Unternehmen für den Datenschutz zuständig ist, wer verantwortlich ist und welche Anforderungen das Unternehmen erfüllen muss. Daneben werden beispielhaft einzelne Maßnahmen vorgestellt, die das Unternehmen bei der Einführung seiner Datenschutzorganisation unterstützend ergreifen kann, um den Herausforderungen, die das Datenschutzrecht an ein Unternehmen stellt, gelassen gegenübertreten zu können.

---

1 Siehe dazu Kapitel 7: *Rath*, Rechtliche Aspekte von IT-Compliance, Ziff 3.2.

2. Verantwortlichkeiten

Das deutsche Datenschutzrecht definiert in § 3 Abs. 7 BDSG (i. V. m. § 2 BDSG) als Verantwortliche die Personen oder Stellen,

- die personenbezogene Daten für sich selbst erheben, verarbeiten oder nutzen oder
- dies durch andere im Auftrag vornehmen lassen.

Eine verantwortliche Stelle hat dafür Sorge zu tragen, dass die durch sie oder ihren Auftragnehmer durchgeführten Datenverarbeitungsvorgänge rechtskonform erfolgen und sie bzw. ihr Auftragnehmer die datenschutzrechtlichen Vorgaben einhält. Verantwortlich ist dabei immer das Unternehmen als juristische Person und nicht etwa nur die Organisationseinheit innerhalb des Unternehmens, die tatsächlich die jeweilige Datenverarbeitung durchführt (bspw. das eigene Rechenzentrum).[2]

Daraus ergibt sich eine besondere Verantwortung der Geschäftsleitung, die in ihrem Unternehmen datenschutzrechtlich relevanten Vorgänge so zu organisieren, dass das Unternehmen insgesamt und speziell die jeweiligen Geschäftsbereiche bzw. Mitarbeiter datenschutzkonform agieren. Dabei sind – entgegen der bislang überwiegenden Praxis[3] – nicht nur die IT-Abteilung oder der CIO einzubinden, sondern alle Geschäftsbereiche, in denen personenbezogene Daten verarbeitet werden. Dazu zählen insbesondere die Bereiche Human Resources, der Vertrieb, das Marketing, der Einkauf, die Buchführung sowie der Betriebsrat und der Betriebsarzt.

Nicht zuletzt hat die Geschäftsleitung sicherzustellen, dass auch Dritte, an die Daten übermittelt werden, den datenschutzrechtlichen Anforderungen Genüge tun. Dies gilt insbesondere, wenn diese Dritten ihren Sitz im Ausland haben und damit die Datenübermittlung und anschließende Verarbeitung speziellen Anforderungen unterliegt.

Eine besondere Verantwortung trifft auch den Datenschutzbeauftragten des Unternehmens: Sofern dieser nach den Vorgaben des BDSG von der Geschäftsleitung zu bestellen ist, hat er als unabhängige Instanz darauf hinzuwirken, dass das Unternehmen seine datenschutzrechtlichen Pflichten erfüllt (vgl. §§ 4f, 4g BDSG).

---

2 Vgl. *Dammann* in: Simitis, BDSG, 5. Aufl. 2003, § 3 Rz. 230 ff.; *Gola/Schomerus*, BDSG, 9. Aufl. 2007, § 3 Rz. 48.

3 Vgl. dazu für Unternehmen der Finanzindustrie: www.compliance-magazin.de/markt/studien/delotitte 051007.html / „Deloitte-Studie vom 05.10.07: Aktuell sollen Identitätsmanamagement, Compliance sowie Disaster Recovery und Business conituity gefördert werden – Ein weiteres herausragendes Thema ist der Datenschutz".

3. Haftung und Rechtsfolgen

3.1 Täterschaft

Wie auch im Rahmen der IT-Compliance[4] haften die Geschäftsleitung, der Datenschutzbeauftragte oder auch einzelne Mitarbeiter für Verstöße gegen datenschutzrechtliche Bestimmungen aus Gesetz bzw. aus entsprechenden Weisungen oder (arbeits-)vertraglichen Vereinbarungen heraus. Verantwortlich ist jeweils derjenige, den die Pflicht, gegen die verstoßen wird, trifft.[5] Hat die Geschäftsleitung daher einer Person eine Pflicht übertragen, haftet diese Person für ihre Verstöße grundsätzlich selbst.[6]

3.2 Ansprüche des Betroffenen

Wird gegen eine Datenschutzbestimmung verstoßen, bspw. durch unerlaubte Weitergabe von Gesundheitsdaten eines Arbeitnehmers an einen potentiellen neuen Arbeitgeber, der dadurch von der Einstellung absieht, und ist dem Betroffenen dadurch ein Schaden entstanden, kann er entsprechende Ansprüche gegen den jeweiligen Täter geltend machen (u. a. gemäß § 7 BDSG, § 823 Abs. 1 und 2 BGB).

Die Praxis zeigt, dass den Betroffenen im Regelfall der Nachweis eines entsprechenden Schadens nur schwer gelingt und daher nur selten tatsächlich Ansprüche auf Schadenersatz geltend gemacht werden. Indes neigen Betroffene immer häufiger dazu, den Datenschutzbehörden vermeintliche Verstöße von Unternehmen zu melden. Die Konsequenz liegt auf der Hand: Die Datenschutzbehörden gehen entsprechenden Hinweisen regelmäßig nach, so dass sich ein Unternehmen in diesem Fall den Nachfragen bzw. Kontrollmaßnahmen der Behörde ausgesetzt sieht.

---

4 Vgl. dazu Kapitel 7: *Rath*, Rechtliche Aspekte von IT-Compliance, Ziff. 2.

5 Vgl. *Ehmann* in: Simitis, BDSG, 5. Aufl. 2003, § 43 BDSG, Rz. 23 ff.

6 Vgl. bspw. für den Fall der Haftung bei fehlender Auskunftserteilung gegenüber einem Betroffenen durch einen Beauftragten: OLG Celle v. 14.6.1995 – 2 Ss (OWi) 185/95, RDV 1995, 244 f.

3.3 Sanktionen der Datenschutzaufsichtsbehörden

3.3.1 Ahndung als Ordnungswidrigkeit

Ein Verstoß gegen Datenschutzbestimmungen kann von den Datenschutzbehörden als Ordnungswidrigkeit mit Bußgeldern bis zu einer Höhe von EUR 250.000,00 geahndet werden (§ 43 BDSG).

Sanktioniert werden zum einen Pflichtverstöße gegen **formelle Pflichten**, die gegenüber den **Datenschutzaufsichtsbehörden** erfüllt werden müssen, wie bspw.

- Verstöße gegen Meldepflichten (§ 43 Abs. 1 Nr. 1 i. V. m. § 4d, Abs. 1, § 4e Satz 2 BDSG),
- Verstöße gegen die Pflicht zur Auskunft (§ 43 Abs. 1 Nr. 10 i. V. m. § 38 BDSG),
- Unterlassen der Bestellung des Datenschutzbeauftragten (§ 43 Abs. 1 Nr. 2 i. V. m. § 4 f Abs. 1 BDSG),

Zum anderen können Pflichtverstöße gegen **formelle Pflichten**, die gegenüber dem **Betroffenen** erfüllt werden müssen, geahndet werden, wie bspw.

- Verstöße gegen Unterrichtungspflichten (§ 43 Abs. 1 Nr. 3 BDSG i. V. m. § 28 Abs. 4 Satz 2, 1. HS BDSG) oder
- Verstöße gegen Benachrichtigungspflichten (§ 43 Abs. 1 Nr. 8 BDSG i. V. m. § 33 Abs. 1 BDSG).

Neben den Verstößen gegen formelle Pflichten werden auch Verstöße gegen **materielle Datenschutzvorschriften** sanktioniert. So werden bspw.

- die unzulässige Übermittlung, Nutzung, Verarbeitung von personenbezogenen Daten oder auch das unbefugte Bereithalten von Daten zum Abruf als Ordnungswidrigkeit geahndet (vgl. § 43 Abs. 1 Nr. 4, Nr. 6, § 43 Abs. 2 BDSG).

3.3.2 Ahndung als Straftat

Erfolgen die in § 43 Abs. 2 BDSG aufgeführten Handlungen, wie die unbefugte Verarbeitung von Daten gegen Entgelt oder mit Bereicherungsabsicht, kann dies als strafbare Handlung geahndet werden und eine Geldstrafe bzw. eine Freiheitsstrafe bis zu zwei Jahren Gefängnis nach sich ziehen (§ 44 BDSG).

3.3.3 Sonstige Maßnahmen

Neben den o.g. Sanktionen dürfen die Datenschutzbehörden die Ausführung der Vorschriften des BDSG im Unternehmen kontrollieren, Auskunft sowie – u. a. unter Verhängung von Zwangsgeld – die Umsetzung von Maßnahmen zur Beseitigung von festgestellten Mängeln technischer oder organisatorischer Maßnahmen verlangen (§ 38 i. V. m. § 43 BDSG).

3.3.4 Verfolgung von Verstößen in der Praxis

In der Vergangenheit haben die Datenschutzbehörden Verstöße weniger mit Bußgeldern und Freiheitsstrafen geahndet, sondern den Schwerpunkt mehr in Richtung Kontrolle und anschließende Beseitigung der Mängel durch das Unternehmen gelegt.[7] Daher ist die Zahl der bis dato in diesem Zusammenhang bekannt gewordenen Entscheidungen als eher gering einzustufen.[8]

Trotzdem sollten sich Unternehmen nicht in Sicherheit wiegen und davon ausgehen, Verstöße würden nicht verfolgt: In der Praxis einigen sich nämlich viele Unternehmen im Laufe der Kontrollmaßnahmen mit den Datenschutzbehörden außergerichtlich. Damit wird zum einen im Sinne der Datenschutzbehörden der Umsetzung der Datenschutzgesetze und dem Gedanken einer künftigen datenschutzgerechten Verarbeitung Rechnung getragen, was naturgemäß für alle Beteiligten vorteilhaft ist. Zum anderen bewahrt dies viele Unternehmen vor einem drohenden Imageverlust. Dessen ungeachtet sollten sich Unternehmen nicht darauf verlassen, dass ihre Verstöße völlig anonym bleiben: Viele Datenschutzbehörden veröffentlichen ihre Tätigkeitsberichte inzwischen online, so dass einer Vielzahl von Interessierten einfach und schnell offen gelegt wird, welche Tätigkeiten die Behörden im Einzelnen entfaltet haben. Auch wenn Unternehmen nicht direkt benannt werden, ist wohl nicht auszuschließen, dass ein interessierter Leser durchaus Rückschlüsse auf das ein oder andere Unternehmen ziehen könnte.[9]

---

7 Vgl. dazu etwa *Weichert*, NStZ 1999, 490.

8 Siehe dazu m. w. N. *Bergmann/Möhrle/Herb*, BDSG, Loseblatt, Stand: Juli 2007, § 43, Rz. 114.

9 Siehe etwa die Tätigkeitsberichte des Hamburgischen Datenschutzbeauftragten unter: http://fhh.hamburg.de/stadt/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/taetigkeitsberichte/start.html.

4. Anforderungen an das Unternehmen

Um datenschutzrechtlich konform Daten in Deutschland zu verarbeiten gilt es einerseits die gesetzlichen Formvorschriften zu beachten und andererseits die Datenverarbeitung an sich gesetzeskonform auszugestalten. Formelle Vorgaben sind direkt von dem Unternehmen zu erfüllen, während der gesetzeskonforme Umgang mit Daten der Mithilfe der Mitarbeiter in ihrer Funktion als datenverarbeitende Person bedarf. Nachfolgend soll kurz dargestellt werden, in welchen Bereichen Unternehmen entweder selbst oder durch ihre Mitarbeiter tätig werden müssen, um datenschutzrechtliche Compliance einzuhalten.

4.1 Formelle Anforderungen

Unternehmen haben formelle Anforderungen sowohl gegenüber den Datenschutzbehörden bzw. dem Datenschutzbeauftragten als auch gegenüber dem Betroffenen, also demjenigen, dessen Daten sie verarbeiten, zu erfüllen. Durch entsprechende Organisationsstrukturen im Unternehmen ist sicherzustellen, dass diese Anforderungen praktisch umgesetzt werden.

4.1.1 Meldung von Verfahren

Gemäß § 4d BDSG sind Unternehmen verpflichtet, vor Inbetriebnahme einer automatisierten Datenverarbeitung der zuständigen Datenschutzaufsichtsbehörde eine Meldung über dieses Verfahren zu machen.[10] Die Meldung muss bestimmte Angaben enthalten, die in § 4e BDSG aufgeführt sind:

- Name des Unternehmens;
- Inhaber, Vorstände, Geschäftsführer oder sonstige Vertretungsberechtigte;
- Anschrift des Unternehmens;
- Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung;
- Beschreibung der von der Verarbeitung betroffenen Personengruppen und der betroffenen Daten oder Datenkategorien;

10 Siehe dazu beispielhaft das Merkblatt zum Meldebogen des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein nebst entsprechender Meldeformulare unter: https://www.datenschutzzentrum.de/wirtschaft/meldung.htm.

- Empfänger oder Empfängerkategorien der Daten (inklusive etwaiger Auftragsdatenverarbeiter);
- Regelfristen für die Löschung der Daten;
- die geplante Datenübermittlung in Drittstaaten (d.h. Länder, die kein den EU-Vorgaben entsprechendes Datenschutzniveau aufweisen, bspw. die USA oder Indien);
- eine allgemeine Beschreibung, die eine vorläufige Beurteilung ermöglicht, ob die ergriffenen technischen und organisatorischen Maßnahmen gemäß § 9 BDSG angemessen sind.

Erfolgt die Meldung nicht rechtzeitig, unvollständig, fehlerhaft oder gar nicht, gilt dies als Ordnungswidrigkeit gemäß § 43 Abs. 1 Nr. 1 BDSG.

Die Meldepflicht **entfällt** gemäß § 4d Abs. 2, 3 BDSG, sofern das Unternehmen

- einen Datenschutzbeauftragten bestellt hat oder
- höchstens neun Personen mit der Datenverarbeitung etc. beschäftigt sind, diese für eigene Zwecke des Unternehmens erfolgt, entweder die Einwilligung desjenigen, dessen Daten verarbeitet werden vorliegt oder die Verarbeitung für Zwecke der Erfüllung eines Vertrages oder vertragsähnlichen Vertrauensverhältnisses erfolgt.

Die Meldepflicht **besteht jedenfalls**, sofern das Unternehmen geschäftsmäßig (also dauerhaft und für wirtschaftliche Zwecke, bspw. Auskunfteien, Adressverlage, Kreditschutzorganisationen wie der SCHUFA)[11] Daten speichert für

- Zwecke der Übermittlung oder
- Zwecke der anonymisierten Übermittlung.

Praxishinweis:

> In der Regel haben Unternehmen Datenschutzbeauftragte bestellt. In diesem Fall ist die Meldung entbehrlich. Handelt es sich jedoch um eine meldepflichtige Auskunftei etc. oder ein Unternehmen, das keinen Datenschutzbeauftragten benötigt, sind Maßnahmen zu ergreifen, die dem Erfordernis der Meldung Rechnung tragen. Die Geschäftsleitung sollte daher zur Minimierung datenschutzrechtlicher Risiken entsprechende organisatorische Maßnahmen einleiten, wie bspw. einen Verantwortlichen in der IT-Abteilung benennen, der die Meldungen vorbereitet und durchführt.

[11] Siehe dazu *Gola/Schomerus*, BDSG, 9. Aufl. 2007, § 29 Rz. 4f.

4.1.2 Erstellen von Verfahrensübersichten

Unternehmen sind verpflichtet, Verfahrensübersichten zu erstellen und ihrem Datenschutzbeauftragten zu übergeben. Der Datenschutzbeauftragte – respektive das Unternehmen, sofern kein Datenschutzbeauftragter zu bestellen ist – haben diese Verfahrensübersicht auf Antrag jedermann zur Verfügung zu stellen (§ 4g Abs. 2 BDSG). Die Verfahrensübersichten enthalten Informationen über die einzelnen Datenverarbeitungsvorgänge im Unternehmen gemäß § 4e Abs. 1 Nr. 1 – 8 BDSG (siehe dazu bereits oben, Ziff. 4.1.1; Angaben zu den technischen und organisatorischen Maßnahmen sind jedoch entbehrlich) sowie die jeweils zugriffsberechtigten Personen. Ändern sich die Datenverarbeitungsvorgänge, sind die Verfahrensübersichten zu aktualisieren.

Praxishinweis:

> Regelmäßig bestehen in Unternehmen erhebliche Defizite sowohl bei der Erstellung als auch bei der Übergabe der Verfahrensübersichten an den Datenschutzbeauftragten. Dies birgt datenschutzrechtliche Risiken, da der Datenschutzbeauftragte gehalten ist, sowohl den Datenschutzaufsichtsbehörden als auch anderen Interessierten die in den Verfahrensübersichten enthaltenen Informationen zur Verfügung zu stellen.
>
> Um diese Defizite auszugleichen, empfiehlt sich die Einrichtung einer entsprechenden Datenschutzorganisationsstruktur: Die Geschäftsbereiche, die mit dem Verfahren in Berührung kommen, bspw. IT und Human Resources, sollten die entsprechenden Angaben proaktiv gemeinsam erarbeiten und dem Datenschutzbeauftragten übergeben. Dies setzt selbstverständlich voraus, dass Verantwortliche benannt werden, die sich der Thematik annehmen.

4.1.3 Vorabkontrolle

§ 4 d Abs. 5, 6 BDSG sieht vor, dass der Datenschutzbeauftragte automatisierte Datenverarbeitungsverfahren vor deren Start zu kontrollieren hat, sofern die Datenverarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen nach sich ziehen kann.[12]

Insbesondere sind Vorabkontrollen durchzuführen, wenn

- besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG), also Daten betreffend die rassische / ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben verarbeitet werden bzw.

---

12 Vgl. zur Durchführung der Vorabkontrolle: *Bergmann/Möhrle/Herb*, BDSG, Loseblatt, Stand: Juli 2007, § 4d, Rz. 46 ff.

- Verarbeitungen durchgeführt werden, die der Bewertung der Persönlichkeit des Betroffenen dienen (insbesondere Fähigkeits-, Leistungs- und Verhaltenskontrollen).

In der Regel unterliegen daher bspw. Personalinformationssysteme, Videoüberwachungssysteme, Scoringdatenbanken der Vorabkontrolle.[13]

Die Vorabkontrolle **entfällt** grundsätzlich, wenn

- das automatisierte Verfahren aufgrund gesetzlicher Vorschriften durchgeführt werden muss,
- eine Einwilligung des jeweiligen Betroffenen vorliegt oder
- die Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder eines vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.

Praxishinweis:

> Selbst wenn die Vorabkontrolle aufgrund der oben genannten Ausnahmen nicht erforderlich sein sollte, empfiehlt sie sich im Regelfall, da so durch den Datenschutzbeauftragten eine Rechtmäßigkeitsprüfung erfolgt, die zumindest die Risiken einer unzulässigen Datenverarbeitung minimieren kann.

Das Unternehmen hat dem Datenschutzbeauftragten für Zwecke der Durchführung der Vorabkontrolle eine Verfahrensmeldung gemäß § 4e Satz 1 BDSG i. V. m. § 4g Abs. 2 BDSG zur Verfügung zu stellen (siehe dazu bereits oben unter Ziff. 4.1.2). Diese Meldung ist Grundlage der Vorabkontrolle.

Der Datenschutzbeauftragte hat bei Zweifeln an der Zulässigkeit der Datenverarbeitung die zuständige Aufsichtsbehörde zu kontaktieren (§ 4d Abs. 6 Satz 3 BDSG). Diese kann in diesem Fall u. a. gemäß § 38 Abs. 1, 3 BDSG Kontrollmaßnahmen im Unternehmen durchführen.

Praxishinweis:

> Der Datenschutzbeauftragte muss in Zweifelsfällen die Datenschutzbehörde benachrichtigen. Ist die Datenverarbeitung unzulässig, so haftet das Unternehmen als verantwortliche Stelle für diesen Verstoß gegen das Datenschutzrecht. Der regelmäßige Austausch zwischen den Beteiligten und der Wille, eine gemeinsame Lösung zu finden, sollten daher als eine dem Datenschutzmanagement immanente Zielsetzung erkannt und gefördert werden. Damit wird das Risiko des reglementierenden Eingriffs einer Behörde in das betriebliche Geschehen zumindest minimiert.

---

[13] Vgl. *Bergmann/Möhrle/Herb*, BDSG, Loseblatt, Stand: Juli 2007, § 4d, Rz. 36 ff.

4.1.4 Bestellung von Datenschutzbeauftragten

Unternehmen, die eine Mindestanzahl von Personen mit der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten beschäftigen, sind grundsätzlich zur Bestellung eines Datenschutzbeauftragten verpflichtet, § 4f BDSG. Ausnahmen bestehen für bestimmte Arten von Datenverarbeitungen, bei deren Durchführung jedenfalls ein Datenschutzbeauftragter bestellt werden muss. Das Unterlassen der Bestellung kann als Ordnungswidrigkeit gemäß § 43 Abs. 1 Nr. 2 BDSG geahndet werden.

Die Verpflichtung besteht **unabhängig von der Anzahl** der mit der Datenverarbeitung beschäftigten Personen, sofern das Unternehmen

- personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung erhebt, verarbeitet oder nutzt (bspw. Auskunfteien, Adressverlage, Markt- und Meinungsforschungsunternehmen; § 4f Abs. 1 S. 6 BDSG) oder
- automatisierte Datenverarbeitungsvorgänge durchführt, die eine Vorabkontrolle gemäß § 4d Abs. 5 BDSG verlangen (z. B. Systeme zur Bewertung der Kreditwürdigkeit, Einsatz von Videoüberwachung, Einführung von Personalinformationssystemen, die eine Persönlichkeitsüberwachung zulassen[14], § 4f Abs. 1 S. 6 BDSG).

Die Verpflichtung besteht **abhängig von der Anzahl** der mit der Datenverarbeitung beschäftigten Personen, sofern das Unternehmen

- mindestens zehn Personen wenigstens vorübergehend mit automatisierter Datenerhebung, -verarbeitung oder -nutzung beschäftigt (§ 4f Abs. 1 S. 4 BDSG) oder
- mindestens zwanzig Personen wenigstens vorübergehend mit nichtautomatisierter Datenerhebung, -verarbeitung oder -nutzung beschäftigt (§ 4f Abs. 1 S. 3 BDSG).

Als Personen zählen sämtliche Beschäftigte, die für das Unternehmen in einem „arbeitnehmerähnlichen Status" tätig werden, also neben den Arbeitnehmern auch Auszubildende, freie Mitarbeiter, Telearbeitnehmer oder auch an die IT des Unternehmens angebundene Handelsvertreter.[15]

Der Datenschutzbeauftragte ist spätestens **binnen eines Monats nach Eintreten der Voraussetzungen schriftlich** zu bestellen; zweckmäßig ist dabei die Festlegung der wichtigsten Aufgaben in der Bestellungsurkunde oder die Bezugnahme auf die Vorschriften der §§ 4f, 4g BDSG. Eine Anzeige der Bestellung gegenüber der Datenschutzaufsichtsbehörde ist nicht erforderlich.

---

14 Vgl. *Bergmann/Möhrle/Herb*, BDSG, Loseblatt, Stand: Juli 2007, § 4d, Rz. 32; *Petri* in: Simitis, BDSG, 5. Aufl. 2003, § 4d, Rz. 32.

15 Vgl. *Däubler*/Klebe/Wedde/Weichert, BDSG, 2. Aufl. 2007, § 4f, Rz. 15 ff.

Dem Unternehmen steht es frei, einen internen oder einen externen Datenschutzbeauftragten zu bestellen.[16] Er hat jedenfalls die nötige fachliche und sachliche Kompetenz und Zuverlässigkeit aufzuweisen, insbesondere sollte er sich im Datenschutzrecht und mit aktuellen Datenverarbeitungstechniken auskennen.[17]

Praxishinweis:

> In der Regel werden Datenschutzbeauftragte aus dem eigenen Unternehmen heraus rekrutiert und üben diese Tätigkeit neben ihrer üblichen Tätigkeit aus. Da der Datenschutzbeauftragte weisungsfrei und unabhängig als Kontrollorgan im Unternehmen agieren muss, sollte davon abgesehen werden, einen Mitarbeiter zu bestellen, der in Interessenkonflikte geraten könnte. Damit sollten insbesondere Leiter der Abteilungen IT, Human Resources und Vertrieb nicht benannt werden. Dies kann auch für Mitarbeiter aus diesen Abteilungen gelten, da in der Konsequenz durch diese Mitarbeiter der Leiter kontrolliert werden müsste. Die Datenschutzaufsichtsbehörde ist berechtigt, die Fachkunde und Zuverlässigkeit zu überprüfen und bei fehlenden Voraussetzungen den Widerruf der Bestellung zu verlangen.

4.1.5 Verpflichtung auf das Datengeheimnis

§ 5 BDSG sieht vor, dass Personen, die bei der Datenverarbeitung beschäftigt sind, mit Aufnahme ihrer Tätigkeit auf die Einhaltung des Datengeheimnisses zu verpflichten sind. Dazu zählt Daten nicht unbefugt zu erheben, zu verarbeiten oder zu nutzen. Ein Verstoß gegen diese Verpflichtung kann arbeitsrechtliche Sanktionen nach sich ziehen; daneben kann die unbefugte Verarbeitung von Daten sowohl für den Täter als auch für das Unternehmen als verantwortliche Stelle zu den oben unter Ziff. 3.2 und 3.3 benannten Konsequenzen führen.

Die Verpflichtung hat persönlich zu erfolgen und muss eine Belehrung über die damit einhergehenden Rechte und Pflichten beinhalten.[18] Zum Nachweis empfiehlt sich eine schriftliche Verpflichtung.[19] Unterbleibt die Belehrung, befindet sich der Beschäftigte ggf. in einem unvermeidbaren Verbotsirrtum und geht ggf. straflos aus.[20] Die Verpflichtung zur Einhaltung des Datengeheimnisses erstreckt sich über das Ende der Tätigkeit hinaus (§ 5 Satz 3 BDSG).

---

16 Vgl. zur Sinnhaftigkeit der Bestellung eines konzernweiten bzw. multinationalen Datenschutzbeauftragten, *Simitis*, BDSG, 5. Aufl. 2003, § 4f Rz. 36 ff.

17 Vgl. zum Berufsbild des Datenschutzbeauftragten LG Ulm, CR 1991, 103, mit Anm. *Ehmann*; *Koch*, Der Betriebliche Datenschutzbeauftragte, 6. Aufl. 2006, S. 131 ff..; *Rudolf*, NZA 1996, 296 ff.

18 Vgl. *Walz,* in Simitis: BDSG, 5. Aufl. 2003, § 5 Rz. 30 f.

19 Dieser kommt insbesondere zum Tragen, wenn dem Mitarbeiter wegen unbefugter Datenverarbeitung arbeitsrechtliche Konsequenzen drohen, vgl. zur Kündigung: LAG Köln v. 29.9.1982 – 5 Sa 514/82, DB 1983, 124 f.; LAG Chemnitz v. 14.7.1999 – 2 Sa 34/99, RDV 2000, 177; VG Frankfurt v. 22.8.2000 – 23 L 1642/00 (V), RDV 2000, 279 ff.; LAG Berlin v. 10.7.2003 – 16 Sa 545/03, RDV 2004, 129 f.

20 Vgl. *Däubler* /Klebe/Wedde/Weichert, BDSG, 2. Aufl. 2007, § 5, Rz. 15.

Der angesprochene Personenkreis ist weit zu fassen: Jeder, der faktisch die Möglichkeit hat, Zugang zu personenbezogenen Daten zu erlangen, ist zu verpflichten.[21] Damit sind nicht nur bspw. Mitarbeiter der Personalabteilung erfasst, sondern auch das Wartungs- oder sogar das Reinigungspersonal.[22]

Praxishinweis:

> Es ist organisatorisch sicherzustellen, dass die entsprechenden Erklärungen eingeholt und archiviert werden. Dabei ist nicht nur die Personalabteilung bspw. bei Einstellung eines Mitarbeiters aufgefordert, eine entsprechende Erklärung einzuholen; auch Abteilungen wie bspw. der Einkauf sollten angewiesen werden, bei bspw. Abschluss eines Wartungsvertrages oder bei der Beauftragung einer Reinigungsfirma Verpflichtungserklärungen zu verlangen.

4.1.6 Technische und organisatorische Maßnahmen

§ 9 BDSG sieht in Verbindung mit der Anlage 1 zu § 9 Satz 1 BDSG verschiedene technische und organisatorische Maßnahmen vor, die es seitens des Unternehmens einzuhalten gilt.[23] In der Regel erfolgt die Umsetzung durch die IT-Abteilung, die die Einhaltung der Maßnahmen in Zusammenarbeit mit dem Datenschutzbeauftragten überwacht.

Selbstverständlich sollte jedes Unternehmen bereits aus Eigeninteresse heraus den höchstmöglichen Sicherheitsstandard anstreben. Da jedoch nicht jede Datenverarbeitung gleich hohe Risiken für die Betroffenen nach zieht, sind nur die Maßnahmen zu ergreifen, deren Umsetzung einen im Verhältnis zu dem angestrebten Schutzzweck angemessenen Aufwand verursacht, § 9 Satz 2 BDSG. Aufwand wird dabei mit Kosten gleichgesetzt.[24] Ein Unternehmen, das bspw. im Rahmen medizinischer Forschung Gesundheitsdaten von Patienten verarbeitet wird strengere – und damit auch kostenintensivere – Maßnahmen ergreifen müssen als ein Unternehmen, das lediglich aus Telefonbüchern Adressen zusammenstellt und an Dritte verkauft. Dabei unterliegt nur der Umfang, aber nie die Umsetzung der Maßnahmen an sich der Verhältnismäßigkeitsprüfung. Fraglich ist daher nie das „Ob" der Umsetzung, sondern nur das „Wie". Die Maßnahmen unterliegen im Übrigen der Kontrolle der Datenschutzaufsichtsbehörden und den entsprechenden Sanktionen (siehe dazu bereits Ziff. 3.3).

---

21 Vgl. *Walz,* in: Simitis, BDSG, 5. Aufl. 2003, § 5 Rz. 14 ff..

22 Vgl. *Walz,* in: Simitis, BDSG, 5. Aufl. 2003, § 5 Rz. 16; *Däubler*/Klebe/Wedde/Weichert, BDSG, 2. Aufl. 2007, § 5, Rz. 5; einschränkend: *Gola/Schomerus*, BDSG, 9. Aufl. 2007, § 5 Rz. 9.

23 Siehe dazu Kapitel 7: *Rath*, Rechtliche Aspekte von IT-Compliance, Ziff. 3.4; Praktische Tipps zur IT-Sicherheit sind bspw. bei dem Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein im Rahmen des IT-Magazins „backUP" unter https://www.datenschutzzentrum.de/backup-magazin/index.htm abrufbar.

24 Vgl. *Ernestus/Geiger,* in: Simitis, BDSG, 5. Aufl. 2003, § 9 Rz. 23 ff.

Praxishinweis:

> Unternehmen sollten vor Aufnahme der jeweiligen Datenverarbeitung eine Risikoanalyse durchführen, welche Datensicherungsmaßnahmen tatsächlich sinnvoll und wirtschaftlich angemessen umsetzbar sind. Die im IT-Grundschutzkatalog des Bundesamtes für Sicherheit und Informationstechnik (BSI) aufgezählten Grundsätze können dabei als Ausgangsbasis für die Umsetzung der mindestens notwendigen Datensicherungsmaßnahmen dienen.[25]

Setzen Unternehmen Auftragnehmer zur Durchführung ihrer Datenverarbeitung ein (so genannte „Datenverarbeitung im Auftrag“ gemäß § 11 BDSG), haben sich die Unternehmen in ihrer Funktion als Auftraggeber davon zu überzeugen, dass der Auftragnehmer ebenfalls die in § 9 BDSG und der Anlage zu § 9 Satz 1 BDSG geforderten Maßnahmen umsetzt, § 11 Abs. 2 BDSG.

Praxishinweis:

> Ist geplant, Datenverarbeitungen durch einen Dritten im Auftrag ausführen zu lassen, bspw. Personalabrechnungen, Inanspruchnahme von Unternehmen zur Durchführung von Rechenzentrumsdienstleistungen, sollte der abzuschließende Auftragsdatenverarbeitungsvertrag eine entsprechende Verpflichtung nebst geeigneten Kontrollmaßnahmen vorsehen.

4.2 Einbindung der Mitarbeiter

Ordnungsgemäße Datenverarbeitung im Unternehmen erfordert nicht nur die Erfüllung der formellen Anforderungen, die das BDSG dem für die Datenverarbeitung Verantwortlichen auferlegt – wesentlich ist selbstverständlich auch die Einhaltung der so genannten „materiellen“ Datenverarbeitungsvoraussetzungen: Das Erheben, Speichern, Verarbeiten und Nutzen von personenbezogenen Daten ist nur unter bestimmten Voraussetzungen erlaubt.

So sieht bspw. § 4 Abs. 1 BDSG vor, dass entweder eine Vorschrift des BDSG oder eine andere Rechtsvorschrift die Verarbeitung bzw. Nutzung erlauben / anordnen muss oder von demjenigen, dessen Daten verarbeitet oder genutzt werden, muss eine entsprechende Einwilligung vorliegen.[26]

---

[25] Siehe dazu bereits Kapitel 7: *Rath*, Rechtliche Aspekte von IT-Compliance, Ziff. 3.4.; Informationen über die IT-Grundschutzkataloge des Bundesamt für Sicherheit in der Informationstechnik sind abrufbar unter folgendem Link: http://www.bsi.de/gshb/deutsch/index.htm; siehe dazu auch: http://www.bsi.de/gshb/baustein-datenschutz/dokumente/b01005_hilfsmittel_tabelle.pdf.

[26] Vgl. bspw. zu den Voraussetzungen der Datenverarbeitung in Unternehmen: *Roßnagel*, Handbuch des Datenschutzrechts, 2003, S. 485 ff.; *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, 4. Aufl. 2005, S. 539 ff.

Gesetzlich erlaubt ist eine Verarbeitung u. a. zur Erfüllung vertraglicher Zwecke, so etwa im Rahmen der Abwicklung von Kundenbestellungen auf der Basis von Kaufverträgen[27] oder auch zur Erfüllung von Zwecken vertragsähnlicher Verhältnisse, bspw. bei der Erhebung von Daten im Rahmen der Vertragsanbahnung oder der Mitgliedschaft in einem Verein (vgl. § 28 Abs. 1 Satz 1 Nr. 1 BDSG).[28] Gesetzlich verboten ist bspw. die Übermittlung von Mitarbeiterdaten ohne deren Einwilligung an einen Adresshändler.

Mitunter setzen die gesetzlichen Erlaubnistatbestände für Datenverarbeitungen Wertungen im Einzelfall voraus: Erlaubt ist eine Datenverarbeitung bspw. dann, wenn die Interessen des Unternehmens an der Übermittlung von Daten höher zu werten sind als die schutzwürdigen Interessen des Mitarbeiters am Unterlassen der Übermittlung (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG bzw. § 28 Abs. 3 Nr. 1 BDSG).[29]

Besonders kritisch ist regelmäßig die Übermittlung von Daten in das außereuropäische Ausland zu werten, da diese grundsätzlich verboten und nur in Ausnahmefällen gestattet ist, §§ 4b, 4c BDSG. Als Ausnahme gelten bspw. die Einwilligung des Betroffenen, die Teilnahme des Datenimporteurs mit Sitz in den USA am so genannten Safe-Harbor-Programm oder der Abschluss von so genannten EU-Standardvertragsklauseln zwischen Datenexporteur und -importeur.[30]

Bereits aus diesen kurzen exemplarischen Beispielen ergibt sich, dass vielfältige Voraussetzungen zu beachten sind, die für jede Fachabteilung sehr unterschiedlich ausgestaltet sein können. Während die Personalabteilung die Verarbeitung von Mitarbeiterdaten ordnungsgemäß gestalten muss, hat die Marketingabteilung vornehmlich Kundendaten zu verwalten.

Das Unternehmen als für die Datenverarbeitung Verantwortlicher hat dafür Sorge zu tragen, dass in jeder Abteilung die vielfältigen materiellen Voraussetzungen erfüllt werden. Es muss sichergestellt sein, dass jeder Mitarbeiter Datenschutzrecht in seiner täglichen Praxis lebt und die Voraussetzungen kennt, unter denen er Daten verarbeiten darf. Damit einhergehend ist das Unternehmen gehalten, seine Mitarbeiter zu schulen und diese in die Lage zu versetzen, die gesetzlichen Anforderungen umzusetzen. Sofern das Unternehmen einen Datenschutzbeauftragten bestellt hat, ist dieser für die Durchführung entsprechender Schulungen verantwortlich.[31]

---

27 Vgl. mit Bsp. zu einzelnen Vertragsverhältnissen: *Bergmann/Möhrle/Herb*, BDSG, Loseblatt, Stand: Juli 2007, § 28, Rz. 21 ff.

28 Vgl. mit weiteren Bsp.: *Bergmann/Möhrle/Herb*, BDSG, Loseblatt, Stand: Juli 2007, § 28, Rz. 193 ff.

29 Vgl. *Bergmann/Möhrle/Herb*, BDSG, Loseblatt, Stand: Juli 2007, § 28, Rz. 217 ff.

30 Siehe dazu bspw. *Gola/Schomerus*, BDSG, 9. Aufl. 2007, § 4c Rz. 4 ff.

31 Siehe zu den verschiedenen Möglichkeiten der Schulung bereits Kapitel 2: *Wecker/Galla*: Pflichten der Geschäftsleitung und Aufbau einer Compliance-Struktur, Ziff. 3.2.2.

Praxishinweis:

> Mittels der Schulung sollen die Mitarbeiter für die Anforderungen des Datenschutzes sensibilisiert werden. Schulungsinhalte können bspw. im Rahmen einer Basisschulung folgende Kernfragen sein:
>
> - Warum ist es notwendig, Datenschutzrecht zu beachten?
> - Wann findet Datenschutzrecht überhaupt Anwendung und was sind personenbezogene Daten?
> - Was ist unter einer automatisierten Datenverarbeitung und -nutzung zu verstehen?
> - Unter welchen rechtlichen Voraussetzungen dürfen Daten verarbeitet werden?
> - Wann und von wem muss eine Einwilligung in die Datenverarbeitung eingeholt werden und welchen Voraussetzungen unterliegt sie?
> - Unter welchen Voraussetzungen darf das Unternehmen Daten für Marketingzwecke verarbeiten?
> - Wann liegt eine Übermittlung von Daten vor und unter welchen Voraussetzungen dürfen Daten an wen übermittelt werden? Sind ggf. vertragliche Vereinbarungen abzuschließen?
> - Welchen Voraussetzungen unterliegt eine Übermittlung ins Ausland, insbesondere in das außereuropäische Ausland?
> - Welche Rechte hat ein Mitarbeiter, ein Kunde etc., dessen Daten durch das Unternehmen verarbeitet werden?
> - Welche technischen und organisatorischen Maßnahmen sind für eine ordnungsgemäße Verarbeitung und Nutzung von Daten einzuhalten?
> - Welche Risiken bestehen bei einer unzulässigen Datenverarbeitung?
>
> Neben der Grundlagenschulung empfiehlt sich eine bereichsspezifische Schulung der Mitarbeiter, bspw. sollten Mitarbeiter aus dem Personalbereich gezielt im Umgang mit Mitarbeiterdaten sensibilisiert werden, während Mitarbeiter im Bereich IT ausführlich im Bereich Umsetzung von technisch / organisatorischen Maßnahmen geschult werden sollten.

Mit Schulung allein ist es jedoch in der Regel nicht getan: Ein gelebtes Datenschutzmanagement setzt auch voraus, dass Mitarbeiter so in eine Datenschutzorganisation eingebunden und so für Datenschutzbelange sensibilisiert werden, dass sie selbstständig erkennen, wann bspw. eine Verarbeitung von Daten zu einem Risiko für das Unternehmen werden könnte und entsprechende Maßnahmen einleiten. In den wenigsten Unternehmen wird bspw. ein reger Austausch zwischen Datenschutzbeauftragten und Mitarbeitern gelebt. Üblicherweise wird der Datenschutz eher als „Hemmschuh“ oder „Erschwernis“ betrachtet und nicht als eine vom

Unternehmen zu lösende Aufgabe, der es genauso wie der Bekämpfung von Korruption oder Diskriminierung zu begegnen gilt. Insofern sollte durch offene Kommunikation dafür Sorge getragen werden, dass die Akzeptanz des Datenschutzes im Unternehmen gestärkt wird, Mitarbeiter Verantwortung tragen, Vorgesetzte den entsprechenden Belangen wohlwollend gegenüberstehen und der Datenschutzbeauftragte Unterstützung erfährt. Nur dann wird eine Datenschutzorganisation entstehen, die dem Unternehmen tatsächlich einen Mehrwert bei der Umsetzung der datenschutzrechtlichen Aufgaben und Gesetze bietet.

4.3 Maßnahmen zur Sicherstellung von Datenschutzcompliance

Neben der Umsetzung der formalen gesetzlichen Vorgaben, der Sensibilisierung und Schulung von Mitarbeitern und Management bieten sich verschiedene Maßnahmen an, die das Unternehmen unterstützend einleiten kann, um Risiken im Bereich des Datenschutzes zu minimieren. Dazu zählen Maßnahmen der Ermittlung des datenschutzrechtlichen Status Quo im Unternehmen, Verpflichtungen der Mitarbeiter zum rechtskonformen Umgang mit Daten oder auch die Möglichkeit, Verstöße zu melden. Letztere Methode ist von besonderer Brisanz, da die Meldung von Verstößen gleichzeitig datenschutzrechtliche Risiken sowohl für den Melder als auch den Meldenden birgt, denen es bei der Einführung entsprechender Systeme – bspw. so genannter „Whistleblowing-Hotlines“, die telefonisch oder online genutzt werden können – zu begegnen gilt.

4.3.1 Datenschutzaudit

Im Rahmen eines Datenschutzaudits werden die in einem Unternehmen bestehenden Datenschutzvorgänge – formeller und / oder materieller Art – überprüft. In der Regel erfolgt eine Bestandsaufnahme des „Ist-Zustands“, der sich eine Gegenüberstellung mit dem „Soll-Zustand“ anschließt, die schließlich in einer Darstellung des im Unternehmen festgestellten Verbesserungsbedarfs nebst anschließender Umsetzung der Verbesserungsvorschläge mündet. In der Praxis hat sich gezeigt, dass ein strukturiertes Datenschutzaudit – ähnlich wie Audits zur Prüfung der Umsetzung von SOX-Anforderungen – erheblich zur Verbesserung der Datenschutzorganisation im Unternehmen beitragen kann.

Eine gesetzliche Verpflichtung zur Durchführung eines Datenschutzaudits besteht indes nicht. § 9a BDSG, der den Gedanken eines formalisierten Audits aufgreift, definiert als Ziel eines Datenschutzaudits die „Verbesserung des Datenschutzes und der Datensicherheit“. Das Datenschutzaudit gilt als Instrument der Selbstkontrolle von Unternehmen und soll einen datenschutzkonformen Umgang mit Daten fördern.[32] Zur Vereinfachung der Durchführung eines

[32] Siehe zu Pro und Kontra eines allgemeinen Datenschutzaudits: *Gola/Schomerus*, BDSG, 9. Aufl. 2007, § 9a Rz. 3 ff.

solchen Audits plant der Gesetzgeber die Einführung des Bundesdatenschutzauditgesetzes (§ 9a S. 2 BDSG), dessen Entwurf seit September 2007 vorliegt.[33] Danach können unabhängige Gutachter die Datenschutzkonzepte und technischen Einrichtungen des Unternehmens einer Prüfung unterziehen, bei deren Erfolg am Ende ein Siegel verliehen werden soll.[34] Ähnliche Konzepte sind bereits auf Länderebene umgesetzt: So bietet bspw. das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein mit seinem Datenschutzgütesiegel die Möglichkeit der datenschutzkonformen Prüfung von IT-Produkten an,[35] daneben gibt es bereits auf Landesebene verschiedene Verfahrensregelungen zur Durchführung von Behördenaudits.[36]

Praxishinweis:

> Neben dem Wettbewerbsvorteil, den ein Unternehmen gegenüber der Konkurrenz durch die Werbung mit einem datenschutzkonformen Produkt bzw. Verfahren sowie seinem Umgang mit Daten erlangen kann, führt ein Audit regelmäßig zu einer veränderten Wahrnehmung des Datenschutzes in Unternehmen: Der Datenschutz und die Verantwortung des einzelnen Mitarbeiters für die von ihm verarbeiteten Daten sowie die aus einer Verletzung des Datenschutzes heraus resultierenden Risiken rücken mehr in den Fokus.
>
> Daneben kann das Unternehmen Schwachstellen konkret identifizieren und eliminieren, im äußersten Fall die für die illegale Verarbeitung Verantwortlichen zur Rechenschaft ziehen.
>
> Im Ergebnis empfiehlt sich die Durchführung eines Audits als Vorstufe zur Einführung einer funktionierenden Datenschutzorganisation. Es sollte zur Sicherstellung des Status Quo regelmäßig wiederholt werden.

4.3.2 Datenschutzrichtlinien

Ein Instrument, um Mitarbeiter in die Datenschutzorganisation einzubinden, ist die Einführung von so genannten „Datenschutzrichtlinien“ oder „Datenschutzpolicies“. In den Datenschutzrichtlinien, die von dem Datenschutzbeauftragten erstellt bzw. geprüft werden sollten, werden Mitarbeiter verpflichtet, bestimmte datenschutzrechtliche Pflichten zu erfüllen und u.a. das geltende Datenschutzrecht zu beachten.

---

33 Vgl. dazu die unter: https://www.datenschutzzentrum.de/bdsauditg/ abrufbaren Materialien.

34 Siehe zu einem möglichen Ablauf eines Audits: *Bizer,* in: Simitis, BDSG, 5. Aufl. 2003, § 9a Rz. 37 ff.

35 Vgl. https://www.datenschutzzentrum.de/guetesiegel/index.htm.

36 Vgl. u.a. § 11c BgfDSG; § 7b BremDSG; § 10a DSG NRW, § 4 Abs. 2 LDSG SH nebst den erforderlichen Ausführungsvorschriften in Schleswig-Holstein (Landesverordnung über ein Datenschutzaudit; GS Schl-H., S. 51, – Gl. Nr. 204-4-2 = RDV 2001, 203 nebst weiterführenden Hinweisen des ULD unter: https://www.datenschutzzentrum.de/audit/material.htm.

Die zu regelnden Bereiche sind vielfältig: Von der allgemeinen Organisationsanweisung, in der der Umgang mit Daten geregelt wird, können Datenschutzrichtlinien auch speziellere Themen betreffen, bspw.

- den Umgang mit Passwörtern,
- die Nutzung von IT-Systemen,
- die Nutzung von Internet, E-Mail und Telefon,
- den Umgang mit Telefax-Geräten,
- die Videoüberwachung,
- die Archivierung und Löschung von Daten oder auch
- Maßnahmen zur Erstellung von Verfahrensverzeichnissen.

Praxishinweis:

> Da diese Richtlinien regelmäßig mehrere Rechtsgebiete betreffen, empfiehlt sich die Prüfung nicht nur durch den Datenschutzbeauftragten, sondern auch eine Prüfung in arbeitsrechtlicher, IT- bzw. Telekommunikationsrechtlicher Hinsicht.
>
> Daneben können Verstöße gegen die Vorschriften in der Regel auch arbeitsrechtliche Konsequenzen nach sich ziehen, so dass sich neben der selbstverständlichen Abstimmung mit dem Management auch die Einbeziehung des Betriebsrats empfiehlt.
>
> Nicht zuletzt sollte die Einhaltung von datenschutzrechtlichen Vorgaben auch ein wesentlicher Bestandteil eines Ethikkodizes oder Code of Conduct sein: Datenschutz ist Ausfluss des allgemeinen Persönlichkeitsrechts und Grundrechtsschutz. Unternehmen sind daher gehalten, sowohl die Persönlichkeitsrechte ihrer eigenen Mitarbeiter als auch die Persönlichkeitsrechte der Personen, deren Daten in ihrem Unternehmen verarbeitet und genutzt werden, umfassend zu wahren. Verbindliche Richtlinien zu einem verantwortungsbewussten Umgang mit Daten sollten daher in keinem Code of Conduct fehlen.

4.3.3 Whistleblowing-Hotlines

Viele Unternehmen haben inzwischen erkannt, dass sie auf Informationen aus dem eigenen Unternehmen angewiesen sind, sofern sie Missstände wie Korruption, Adresshandel, Betrug etc. erfolgreich und schnell aufdecken wollen. Daneben erfordert die Umsetzung der Vorgaben aus den nun immer häufiger auch in Deutschland eingeführten Ethikkodizes einen Kontrollmechanismus betreffend die Umsetzung der dort statuierten Regelungen. Eine schnelle

Aufdeckung von Verstößen ist für Unternehmen nicht nur aus Eigeninteresse notwendig: Handelt es sich um Unternehmen, die selbst oder deren Muttergesellschaft an US-Börsen notiert sind, sind sie dazu sogar durch die Vorgaben des Sarbanes-Oxley-Acts[37], verpflichtet.

Ein Instrument zur Aufdeckung von Missständen sind die so genannten „Whistleblowing-Hotlines", die telefonisch oder online durch Unternehmen, häufig mit Unterstützung darauf spezialisierter Call-Center, Ombudsmänner und / oder Datenverarbeiter, betrieben werden.

„Whistleblowing" bedeutet übersetzt „in die Pfeife blasen, auf etwas aufmerksam machen". Daraus leitet sich bereits der Zweck dieser Hotlines ab: Mitarbeiter können über die Hotline das Fehlverhalten anderer anzeigen. Naturgemäß birgt eine solche Hotline die Gefahr der Denunziation Unschuldiger; sie weist jedoch auch datenschutzrechtlich eine erhebliche Brisanz auf: Während in den USA das Datenschutzrecht eher zurückhaltend ausgestaltet ist und daher wenig rechtliche Bedenken gegenüber der Erhebung, Speicherung und Verarbeitung von Daten des Meldenden und des Gemeldeten bestehen, gestaltet sich die Rechtslage in Europa anders. Der Schutz des Einzelnen und seiner Persönlichkeitsrechte vor dem Missbrauch seiner Daten durch bewusste Falschanzeigen oder auch die Möglichkeit der Rückverfolgung des Melders nebst damit für diesen einhergehenden Risiken wird im Vergleich zu den USA wesentlich höher gewertet. Die Interessen des Unternehmens an einer raschen Aufklärung der Missstände überwiegen aus europäisch geprägter datenschutzrechtlicher Sicht nicht automatisch die Interessen des Einzelnen und scheitern mitunter an den Datenschutzgesetzen der einzelnen europäischen Länder. Dies gilt insbesondere, wenn im Rahmen der Hotline ein umfassender Datenaustausch zwischen diversen Beteiligten mit Sitz innerhalb und außerhalb der EU stattfindet.

Um Unternehmen nicht in die unhaltbare Situation zu bringen, im Gebiet der EU eine Hotline auf Grundlage der SOX-Vorgaben betreiben zu müssen, die nach den jeweiligen europäischen Vorgaben verboten ist,[38] hat die Art. 29-Gruppe, die sich aus den Datenschutzbeauftragten der EU-Mitgliedstaaten zusammensetzt, eine Stellungnahme betreffend die datenschutzrechtliche Zulässigkeit des Betriebs einer solchen Hotline innerhalb des Gebiets der EU abgegeben.[39] Parallel haben auch andere Datenschutzbehörden in Europa entsprechende Empfehlungen bzw. sogar Registrierungs- oder Anzeigepflichten erlassen, die vor der Inbetriebnahme einer Hotline zu erfüllen sind.[40] Wesentliches Ziel sämtlicher Bestrebungen ist es dabei, sowohl den Gemeldeten als auch den Melder ausreichend zu schützen und einen unkontrol-

---

[37] Abrufbar unter: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf.

[38] Vgl. bspw. die Entscheidungen der französischen Datenschutzbehörde CNIL, CNIL Entscheidung 2005-110 v. 26.5.2005 (Mc Donald's Gruppe Frankreiche); CNIL Entscheidung 2005-111 vo. 26.5.2005 (Exide Technologies) oder auch die Entscheidung des LAG Düsseldorf v. 14.11.2005 – 10 TaBV 46/05, BB 2006, 335 betreffend die Mitbestimmung bei Einführung einer Ethikrichtlinie im Fall Wal-Mart.

[39] Abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf.

[40] Vgl. bspw. unter: http://www.cnil.fr/fileadmin/documents/uk/CNIL-recommandations-whistleblowing-VA.pdf. oder die Empfehlungen des Düsseldorfer Kreises für den Betrieb von Hotlines in Deutschland, abrufbar unter: http://fhh.hamburg.de/stadt/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/informationsmaterial/wirtschaft/whistleblowing-pdf,property=source.pdf.

lierten Datenfluss überflüssiger und diskriminierender Daten zu verhindern. Die Empfehlungen umfassen daher u.a. den Inhalt der Meldungen, den Umgang mit den Meldungen, die Zugriffsberechtigungen, die Meldebefugnisse, den Personenkreis, der gemeldet werden darf oder auch die bestehenden Informationspflichten gegenüber Mitarbeitern, Melder und Gemeldetem.[41]

Praxishinweis:

> Unabhängig von dem Imageschaden, den ein Verstoß von Unternehmen gegen datenschutzrechtliche Vorgaben nach sich zieht, scheuen sich die Datenschutzbehörden auch nicht Bußgelder zu verhängen und die Umsetzung ihrer Vorgaben bei Einführung einer Hotline zu kontrollieren. Insofern empfiehlt es sich vor Einführung einer entsprechenden Hotline sorgfältig zu prüfen, ob diese nach den jeweiligen landesspezifischen Vorgaben zulässig ist bzw. ob Registrierungs- oder Anzeigepflichten bestehen und die jeweiligen Datenströme rechtlich zulässig ausgestaltet sind.

5. Fazit

Während die formellen Voraussetzungen, die das deutsche Datenschutzrecht den Unternehmen auferlegt, relativ einfach umzusetzen sind, gestaltet sich die Einführung einer funktionsfähigen Datenschutzorganisation in der Regel etwas komplizierter. Alle Beteiligten sind über ihre eigene Verantwortung aufzuklären, in die Organisation einzubinden und so zu sensibilisieren, dass sie aus eigenem Antrieb für einen rechtskonformen Umgang mit Daten Sorge tragen.

Selbstverständlich obliegt dem Datenschutzbeauftragten als dem maßgeblichen Kontrollorgan im Unternehmen dabei eine wesentliche Verantwortung. Dazu bedarf er aber der Unterstützung des Managements. Nur dann, wenn auch das Management die Anforderungen des Datenschutzes nicht als „Hemmnis“ sondern als notwendige Maßnahmen zur Wahrung der Rechte des Einzelnen und als Chance, sich gegenüber dem Wettbewerb wohltuend abzuheben begreift, wird eine Datenschutzorganisation mit Leben gefüllt.

---

[41] Vgl. dazu weitergehend: *Wisskirchen/Körber/Bissels*: Whistleblowing und Ethikhotlines, BB 2006, 28 ff.; *Breinlinger/Krade*r: Whistleblowing – Chancen und Risiken bei der Umsetzung von anonym nutzbaren Hinweisgebersystemen im Rahmen des Compliance-Managements von Unternehmen, RDV 2006, 1 ff.

Dabei sollte das Management nicht außer Acht lassen, dass Datenschutz ein wesentlicher Bestandteil von „Unternehmens-Compliance“ ist und Verstöße gegen die entsprechenden gesetzlichen Vorgaben Haftungsfolgen sowohl für das Unternehmen als auch für das Management selbst nach sich ziehen können. Nicht vergessen werden darf weiterhin, dass der Datenschutz immer stärker in den Fokus der Öffentlichkeit gerät. Damit einhergehend registriert der Einzelne mit Interesse, wie mit seinen Daten bei welchem Unternehmen umgegangen wird. Unternehmen werden daher immer häufiger mit Anfragen und Ansprüchen von Betroffenen konfrontiert oder auch von Datenschutzbehörden kontrolliert. Eine funktionierende Datenschutzorganisation hilft, diesen Anforderungen gelassen entgegenzusehen.

IP-Compliance

Detlef Mäder

Zusammenfassung

IP-Compliance betrifft den Bereich gewerblicher Schutzrechte (z. B. Marken, Patente, Geschmacksmuster) und Urheberrechte sowie weitere Rechte geistigen Eigentums (z. B. Betriebsgeheimnisse und Know-How). Ein mögliches Haftungsrisiko für betroffene Unternehmen kann sich z. B. aus der Verletzung fremder Schutzrechte und daraus resultierender Unterlassungs-, Auskunfts-, Schadensersatz und Vernichtungsansprüche ergeben.[1] Zudem kann die Reputation des jeweiligen Unternehmens beschädigt werden. Darüber hinaus stellen IP-Rechte einen oft wesentlichen Vermögenswert des Unternehmens dar.

1. „Best Practice“ für IP-Compliance

Zunächst sollte eine Analyse der bestehenden Schutzrechte durchgeführt werden. Im Anschluss hieran bietet sich eine Bewertung der Relevanz und daraus hervorgehende Abstufung an. Unter Zugrundelegung der so gewonnenen Erkenntnisse kann eine unternehmensinterne IP-Richtlinie geschaffen werden. Diese könnte in der Folgezeit implementiert und überwacht werden.[2]

---

1 *Krieger/Uwe H. Schneider*, Handbuch Managerhaftung, 2007, § 21 Rn. 3 ff.

2 Vgl. Compliance-Magazin.de „Deloitte-Studie: Optimale Nutzung geistigen Eigentums braucht Intelligentes Management“.

2. IP-Richtlinie

Eine unternehmensinterne IP-Richtlinie muss Handlungsanweisung für den Schutz unternehmenseigener IP-Assets und Regelungen zur Vermeidung von Konflikten mit Schutzrechten Dritter enthalten.[3]

Darüber hinaus müssen Arbeitsabläufe und Prüfungsprozesse für den Schutz und die Verwendung eigener IP-Assets beschrieben werden. Hervorzuheben ist beispielsweise, dass Marken- und Patentrecherchen im Vorfeld einer Nutzung solcher IP-Rechte durchgeführt werden sollten, um Haftungsrisiken wegen etwaiger Schutzrechtskollisionen zu reduzieren. Denkbar sind auch verschiedene Schutzstrategien je nach Relevanz der IP-Assets. Dabei kann sich im Einzelfall ein Konflikt zwischen einem frühzeitigen Schutz eines solchen IP-Rechts und einer so erfolgenden frühzeitigen Information bzw. Offenlegung gegenüber Wettbewerbern ergeben. Zudem gilt es, den genauen Schutzumfang zu definieren, d. h. die geografische und inhaltliche Erstreckung des jeweiligen Schutzrechts.

Im Rahmen der IP-Richtlinie ist auch die Überwachung der bestehenden Schutzrechte und die entsprechende Marktbeobachtung zu regeln. Des Weiteren gilt es, den Bereich des Lizenzvertragsmanagements und der Verwaltung entsprechender vertraglicher Vereinbarungen festzulegen. Ein weiteres, in der IP-Richtlinie zu regelndes Feld sind Handlungsanweisungen für den Erwerb/die Lizenzierung fremder Schutzrechte. Diese kommen beispielsweise beim Einkauf von Content für Websites, Kreativleistungen jeder Art und Erfindungen zur Anwendung. Die Verwendung von Software und Open-Source-Anwendungen ergeben eine Schnittstelle zur IT-Compliance.

Letztlich ist in der IP-Richtlinie ein Verfahren für die frühzeitige Einbindung und Abstimmung aller betroffenen Unternehmensbereiche vorzusehen. Dies sind beispielsweise Rechtsabteilung, Forschungs- und Entwicklungsabteilung, Marketing, Vertrieb und Business-Development.

Die spätere Implementierung und Überwachung der IP-Compliance setzt zunächst ein Commitment der Unternehmensleitung voraus, diese Abläufe zu überwachen und zu begleiten. Zudem sind Schulungen und die Gewährleistungen des Informationsflusses sicherzustellen, ggf. sind spätere Anpassungen der Richtlinie notwendig, um ihre Umsetzung sicherzustellen.

---

3 Vgl. Compliance-Magazin.de „Verhaltenskodex bei BASF“ v. 20.12.2006.

3. Unternehmenskommunikation und IP-Compliance

Auch im Bereich der Unternehmenskommunikation können sich Compliance-Fälle ergeben. Beispielhaft sei hier der Fall „Kirch ./. Breuer“[4] genannt, der ein klassisches Beispiel dafür ist, dass keine ausreichende vorherige Prüfung der Unternehmenskommunikation erfolgt ist. Unternehmenskommunikation in diesem Sinne betrifft jedoch nicht nur die externe, sondern auch die interne Form der Kommunikation. Beispielhaft seien hier als mögliche zu betrachtende Anwendungen Interviews, Presseerklärungen, Kundenzeitschriften, Newsletter, das Internet, Mitarbeiterzeitschriften, aber auch das Intranet genannt.

Ansprüche in diesem Zusammenhang können sich sowohl aus zivilrechtlichen und strafrechtlichen Normen, als auch dem Presse- und Wettbewerbsrecht ergeben.

Insbesondere neue Kommunikationsformen wie Corporate Blogs, Internet-Foren und Podcasts bieten vielfältige Möglichkeiten, in denen Risiken im Hinblick auf die Unternehmens-Compliance entstehen können. Insoweit gilt es auch, Mitarbeiter anzuhalten, wie solche Kommunikationsformen zu nutzen sind und welche Äußerungen getätigt werden dürfen.

Compliance-Maßnahmen im Bereich der Kommunikation können beispielsweise auch darin bestehen, auch die Unternehmenskommunikation und Marketing/Sales durch die Gestaltung einer Richtlinie zu regeln. Dabei gilt es jedoch, die Gratwanderung zwischen konkreter Handlungsanleitung und einer Überfrachtung zu meistern, da in diesem Bereich konkrete Anforderungen nur schwer möglich sind. In jedem Falle sollten auch Zulieferer, Subunternehmer, etc. entsprechend in den Bereich der Unternehmenskommunikation bzw. einer entsprechenden Compliance-Richtlinie einbezogen werden.

4 BGH v. 24.01.2006 – XI ZR 384/03, NJW 2006, 830 ff.

Kartellrechts-Compliance

Helmut Janssen

Zusammenfassung

Eine funktionierende Kartellrechts-Compliance vermeidet oder verringert im Wesentlichen folgende Risiken: drastische Bußgelder gegen das Unternehmen und damit Wertminderung des Unternehmens, Bußgelder gegen Vorstand, Geschäftsführung und Mitarbeiter, Schadenersatzansprüche gegen Unternehmen und Mitarbeiter, Störung der betrieblichen Abläufe durch Ermittlungsverfahren, Strafverfolgung und Haftstrafen im In- und Ausland. Dabei ist eine Kartellrechts-Compliance in vielen Unternehmen ohne größeren organisatorischen Aufwand möglich. Oft genügen eine intelligente Organisation der Mitarbeiter, regelmäßige Schulungen sowie einige überschaubare Verhaltensregeln. Auch wenn bei einzelnen Unternehmen, je nach Größe und Branche, der Aufwand größer sein kann: er wird sich zum Schutz der Führung, der Mitarbeiter und der Eigentümer des Unternehmens stets lohnen. Zumindest muss die Kartellrechts-Compliance der Unternehmensleitung vor Augen führen, wo Risiken im eigenen Unternehmen liegen, wie sie zu bewerten sind und wie mit ihnen umgegangen werden kann.

1. Ziele der Kartellrechts-Compliance

- Warum braucht man Compliance, und wer braucht sie? -

Ziel kartellrechtlicher Compliance ist es, Nachteile für das Unternehmen, seine Mitarbeiter und seiner Gesellschafter dadurch auszuschließen oder zu verringern, dass man Verstöße gegen das Kartellrecht vermeidet und im Fall von Verstößen richtig reagiert. Dazu werden zunächst jene Risikobereiche skizziert, die eine kartellrechtliche Compliance eingrenzen muss (dazu 2). Danach werden die Nachteile beschrieben, die dem Unternehmen, seinen Managern, seinen Arbeitnehmern und seinen Gesellschaftern bei einem Verstoß gegen das Kartellrecht drohen (dazu 3). Im Anschluss wird dargestellt, welche dieser Nachteile eine kartellrechtliche Compliance – ganz oder zum Teil – ausschließen kann (dazu 4). Abschließend werden Bestandteile eines effektiven Compliance Programms erläutert (dazu 5).

2. Risikobereiche im Unternehmen

- Was ist haftungsträchtig und verboten? -

Um den Aufwand für die Kartellrechts-Compliance in ein vernünftiges Verhältnis zum Risiko zu setzen, wird man zunächst betrachten, ob bestimmte Bereiche ausgegrenzt werden können. So ist etwa zu fragen, ob das Unternehmen mit einem seiner Produkte oder Dienstleistungen Marktbeherrscher ist. Denn für einen Marktbeherrscher gelten strengere Regeln, wenn er einseitig (d.h. ohne Abstimmung mit seinen Wettbewerbern) zum Beispiel Preise festsetzt, Rabatte gewährt oder Vertriebsbindungen auferlegt. Auch gibt es Unternehmen, deren Wert nicht unwesentlich von der Wirksamkeit bestimmter Vertriebsvereinbarungen abhängt, zum Beispiel von einer geografischen Exklusivität oder einer langfristigen Alleinvertriebsvereinbarung. Während beim Marktbeherrscher die Compliance bereits im Prozess der Preis- und Konditionenbildung einsetzen muss, würde im Beispiel der Vertriebsbindungen eher das laufende Vertragsmanagement gefragt sein. In den meisten Fällen werden kritische Formen der Koordination mit Wettbewerbern Gegenstand der Kartellrechts-Compliance sein. Dies sind:

- klassische Kartellabsprachen mit Wettbewerbern. Also die Absprache von Preisen und Quoten und die Aufteilung von Gebieten und Kundengruppen.[1]
- gewisse Formen des Informationsaustausches. So sind nach der Rechtsprechung etwa Marktinformationssysteme problematisch, wenn sensible, genaue und aktuelle Daten in kurzen zeitlichen Abständen gemeldet und nicht hinreichend aggregiert und anonymisiert werden.[2]
- der Missbrauch einer marktbeherrschenden Stellung. Zum Beispiel ist die Deutsche Telekom 2003 wegen unangemessener Preise im Ortsnetz von der Europäischen Kommission bebußt worden.[3] Der Microsoft-Fall[4] hat über längere Zeit Schlagzeilen in der Tagespresse gemacht.
- der Aufruf zum Boykott. Einen solchen Vorwurf hatte das Bundeskartellamt zum Beispiel gegen das Duale System Deutschland (DSD) erhoben.[5]

---

1 Vgl. *von Dietze/Janssen*, Kartellrecht in der anwaltlichen Praxis, 3. Aufl. München 2007, Rn. 146; Aktuelles Beispiel: Unternehmen, die Privat- und Gewerbekunden mit Flüssiggas beliefern, verständigen sich darauf, sich gegenseitig keine Kunden abzuwerben; wechselwilligen Kunden wird auf Nachfrage kein Preis oder ein abschreckend hoher Preis genannt; wechselt der Kunde dennoch den Lieferanten, informieren sich die Unternehmen und zahlen untereinander einen Ausgleich. Pressemitteilung des BKartA vom 19. Dezember 2007.

2 Vgl. etwa EuG v. 5.5.2001, Rs. T-16/98 – Wirtschaftsvereinigung Stahl gegen Kommission. *Zimmer*, in: Immenga/Mestmächer, GWB, 2. Aufl. 2007, § 1 Rn. 303 ff.

3 EG-Kommission vom 21. Mai 2003, ABl EG Nr. L 263/9.

4 Microsoft gegen Kommission, EuG v. 17.9.2007, Rs. T 201/04.

5 Siehe Pressemitteilung des BKartA vom 23. Januar 2003.

- Es gibt noch andere Verbote, die im Weiteren nicht sonderlich interessieren. Sie untersagen im Wesentlichen Falschangaben, die bei Fusionskontrollverfahren, also bei Unternehmenszusammenschlüssen, gegenüber dem Bundeskartellamt oder der Kommission gemacht werden. Billig sind auch solche Verstöße nicht. Das Bundeskartellamt hat in der INVISTA-Entscheidung 250.000 Euro[6] verhängt.

Im Unternehmen bewegen sich vor allem Vorstände, Geschäftsführer und Vertriebsleiter in diesen Risikobereichen.

Das Risiko entdeckt zu werden, ist nicht zu unterschätzen. Kartelle werden in der Regel dadurch aufgedeckt, dass ein beteiligtes Unternehmen einen Kronzeugenantrag bei einer Kartellbehörde (oder bei mehreren) stellt, um auf diese Weise eine Geldbuße zu vermeiden oder zu verringern (die Bayer AG hat auf diese Weise zuletzt 201 Millionen Euro gespart[7]). Auslöser für einen solchen Kronzeugenantrag ist oft, dass ein Unternehmen verkauft wird und der neue Eigentümer eine Geldbuße zu Lasten dieses Unternehmens oder eine Haftung seiner Geschäftsführer ausschließen will. In jedem Mustervertrag für einen Unternehmenskauf dürfte heutzutage die Garantieerklärung des Verkäufers enthalten sein, die Zielgesellschaft habe das Kartellrecht befolgt. Überdies haben viele Kartellbehörden in den vergangenen Jahren Abteilungen eingerichtet, die selbst ermitteln und verfolgen (beim Bundeskartellamt die „Sonderkommission Kartellbekämpfung“), oft auch in Zusammenarbeit mit Behörden anderer Staaten.[8] Allein bei der Europäischen Kommission arbeiten 70 Inspektoren („Kartelljäger“) in diesem Bereich.[9] Daneben erhöhen auch die Untersuchung bestimmter Wirtschaftszweige durch die Kommission (sog. Sektoruntersuchung[10]), ein Wechsel des Geschäftsführers oder das unfreiwillige Ausscheiden eines Mitarbeiters das Entdeckungsrisiko für die Mitglieder eines Kartells.

---

6 Siehe Pressemitteilung des BKartA vom 5. Oktober 2005.

7 Obgleich sie als Wiederholungstäter dingfest gemacht worden war! Pressemitteilung der Kommission IP/07/1855 vom 5. Dezember 2007.

8 Gegen Hersteller von Flachglas verhängte die Kommission eine Geldbuße in Höhe von EUR 486,9 Mio. nach eigenen Ermittlungen, die sie auf der Grundlage von Informationen durch mitgliedstaatliche Kartellbehörden eingeleitet hatte; vgl. Pressemitteilung IP/07/1781 vom 28. November 2007.

9 Die Kommission leitete ein Verfahren eigeninitiativ gegen Hersteller professioneller Videobänder ein, das sie im November 2007 mit der Verhängung einer Geldbußen in Höhe von 74 Millionen Euro abschloss; vgl. Pressemitteilung der Kommission IP/07/1725 vom 20. November 2007.

10 Die Kommission hat am 16. Januar 2008 zum ersten Mal im Rahmen einer Sektoruntersuchung unangekündigte Nachprüfungen in den Geschäftsräumen von Pharma-Herstellern durchgeführt, also ohne dass konkrete Indizien für einen Verstoß vorlagen; vgl. Pressemitteilung IP/08/49 vom 16. Januar 2008.

3. Drohende Nachteile

- Was droht wem? -

3.1 Drastische Bußgelder gegen Unternehmen

Kommission und Kartellamt können nach europäischem bzw. deutschem Recht jedem an einem Verstoß beteiligten Unternehmen Bußgelder bis zu 10 % des jeweiligen weltweiten Gesamtumsatzes auferlegen.[11] Gemeint ist damit der Konzernumsatz der beteiligten Unternehmen, d.h. im Falle eines abhängigen Unternehmens kommt es auf die Umsätze der herrschenden Unternehmen sowie der von ihnen abhängigen Unternehmen an.[12] Im Jahr 2007 hat allein die Europäische Kommission Geldbußen über mehr als 3,3 Milliarden Euro verhängt (Stand 5. Dezember 2007). So entfiel zum Beispiel auf Thyssen Krupp für seine Beteiligung am „Aufzugskartell" ein Bußgeld in Höhe von 479.669.850 Euro.[13] Eine neue Berechnungsweise wird in Zukunft die Geldbußen weiter ansteigen lassen.[14]

Bußgelder sind grundsätzlich nicht als Betriebsausgaben steuerlich abzugsfähig.[15] Dies gilt aber dann nicht, „soweit der wirtschaftliche Vorteil, der durch den Gesetzesverstoß erlangt wurde, abgeschöpft worden ist, wenn die Steuern vom Einkommen und Ertrag, die auf den wirtschaftlichen Vorteil entfallen, nicht abgezogen worden sind."[16]

---

11 § 81 Abs. 4 Satz 2 GWB, Art. 23 Abs. 2 VO 1/2007. Adressat des Verbotes und der Bußgeldvorschrift ist nach europäischem Recht das Unternehmen. Das Verhalten der natürlichen Person wird dem Unternehmen als eigenes schuldhaftes Handeln zugerechnet. Das deutsche Recht rechnet dem Unternehmen über § 30 OWiG das Handeln von Unternehmensangehörigen und über §§ 130, 30 OWiG die Aufsichtspflichtverletzung des gesetzlichen Vertreters zu.

12 Gegen die Einbeziehung von Umsätzen, die Unternehmen erzielen, die mit dem beteiligten Unternehmen verbundenen sind, *Bechtold*, in: Bechtold, GWB, 4. Aufl. 2006, § 81 Rn. 27.

13 Pressemitteilung der Kommission IP/07/209 vom 21. Februar 2007.

14 Leitlinien für das Verfahren zur Festsetzung von Geldbußen gemäß Artikel 23 Absatz 2 Buchstabe a) der Verordnung (EG) Nr. 1/2003, ABl. EU 2006 Nr. C 210, S. 2.

15 § 4 Abs. 5 Satz 1 Nr. 8 Satz 1 EStG.

16 § 4 Abs. 5 Satz 1 Nr. 8 Satz 4 EStG.

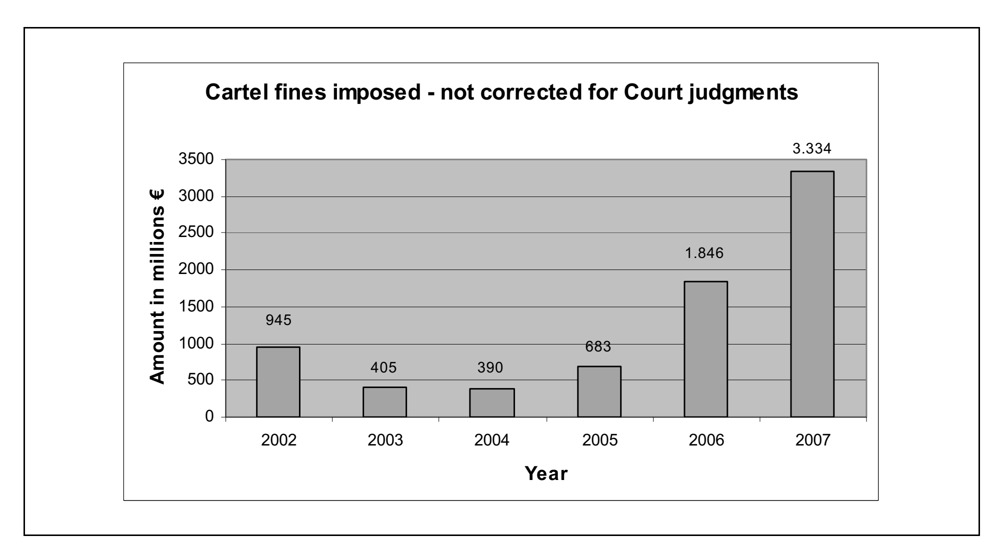


Abbildung 1: *Von der Europäischen Kommission verhängte Geldbußen (seit 2002)*[17]

Year	Untertaking	Case	Amount in EUR*
2007	ThyssenKrupp	elevators and escalators	479.669.850
2001	F. Hoffmann-La Roche AG	Vitamins	462.000.000
2007	Siemens AG	gas insulated switchgear	396.562.500
2006	Eni SpA	synthetic rubber	272.250.000
2002	Lafarge SA	Plasterboard	249.600.000
2001	BASF AG	Vitamins	236.845.000
2007	Otis	elevators and escalators	224.932.950
2007	Heineken NV	dutch beer market	219.275.000
2006	Arkema SA	Methacrylates	219.131.250
2006	Solvay SA / NV	hydrogen peroxide	167.062.000

Tabelle 1: *Top Ten der bebußten Unternehmen (nur Europäische Kommission)*[18]

17 http://ec.europa.eu/comm/competition/cartels/statistics/statistics.pdf.

18 http://ec.europa.eu/comm/competition/cartels/statistics/statistics.pdf.; am 27.2.2008 hat die Kommission (vgl. Pressemitteilung der Kommission IP/08/318 vom 27. Februar 2008) gegen Microsoft ein Zwangsgeld in Höhe von EUR 899.000.000 verhängt. Mit dieser Entscheidung hat die Kommission gezeigt, dass sie auch die Nichterfüllung von Auflagen, die sie in einer früheren Entscheidung gegen das Unternehmen festgelegt hat, nicht hinnimmt.

3.2 Bußgelder gegen natürliche Personen – Vollstreckung in das Privatvermögen

Nach deutschem Recht können Bußgelder nicht nur gegen Unternehmen, sondern auch gegen natürliche Personen verhängt werden. Das Bundeskartellamt macht von dieser Befugnis regelmäßig Gebrauch. Die Europäische Kommission kann in aller Regel keine Bußgeldentscheidung gegen eine natürliche Person treffen.[19] Allerdings sind die deutschen Kartellbehörden befugt und verpflichtet, europäisches Recht durchzusetzen. Somit kann das Bundeskartellamt bei einem Verstoß gegen europäisches Kartellrecht nach den Vorschriften des OWiG auch gegen natürliche Personen Bußgelder festsetzen. Für den Betroffenen ist damit von entscheidender Bedeutung, ob ein Verfahren vom deutschen Kartellamt oder von der Europäischen Kommission geführt wird.

Die Höhe des Bußgeldes gegen eine natürliche Person ist auf 1 Million Euro für jeden einzelnen Verstoß begrenzt.[20] Für weniger gravierende Verstöße liegt die Obergrenze bei 100.000 Euro.[21] Bei klassischen Kartellen, also Absprachen über Preise, Gebiete, Quoten und Kundenaufteilung werden die Kartellbehörden praktisch immer von einem gravierenden Verstoß ausgehen. Einen weniger gravierenden Verstoß wird man in der Praxis wohl nur bei unvollständiger Anmeldung eines Unternehmenszusammenschlusses annehmen.

Versichern lässt sich das Risiko des Einzelnen in der Regel nicht. D&O-Versicherungen (Directors and Officers Liability Insurance) enthalten zumeist ausdrückliche Haftungsausschlüsse. Bußgelder sind auch nach den Allgemeinen Versicherungsbedingungen für die Vermögensdschaden-Haftpflichtversicherung von Aufsichtsräten, Vorständen und Geschäftsführern (AVB-AVG) von 1997 nicht vom Versicherungsschutz umfasst. Schließlich entfällt bei vorsätzlich begangenen Verstößen der Versicherungsschutz bereits auf Grund von § 61 VVG.

Bußgeldpflichtig werden können Personen durch ihr eigenes Handeln (unmittelbar Handelnde und Beteiligte; dazu sogleich unter 3.3) oder durch die Verletzung ihrer Aufsichtspflicht (dazu 3.4).

---

19 Auch nach europäischem Recht könnte eine natürliche Person bebußt werden, wenn sie selber als „Unternehmen" im Sinne des EG-Kartellechts zu qualifizieren wäre.

20 § 81 Abs. 4 Satz 1 GWB.

21 § 81 Abs. 4 Satz 3 GWB.

3.3 Handelnde Personen

Über § 9 OWiG kann den unmittelbar handelnden Personen die Unternehmenseigenschaft der kartellrechtlichen Verbotsnorm zugerechnet werden. Dies sind in der Regel gesetzliche Vertreter und zu eigenverantwortlicher Aufgabenerledigung beauftragte Personen wie der Leiter einer Vertriebsabteilung oder einer Rechtsabteilung.[22] Mittelbare Täterschaft, Anstiftung und Beihilfe gibt es im Ordnungswidrigkeitenrecht nicht. Bußgeldpflichtig können auch die „sonstigen Beteiligten" (§ 14 Abs. 1 Satz 2 OWiG) sein – demnach macht sich jeder bußgeldpflichtig, der den Handelnden „im Bewusstsein des Kartellrechtsverstoßes bei der Organisation eines Preiskartells unterstützt".[23] In der Praxis konzentriert sich das Bundeskartellamt auf die Entscheider im Unternehmen.

3.4 Aufsichtspflichtige

Gemäß § 130 OWiG kann ein Bußgeld auch gegen aufsichtspflichtige Personen verhängt werden. Dies setzt zum einen voraus, dass der Aufsichtspflichtige nicht bereits als Handelnder (§ 9 Abs. 2 OWiG) bebußt wird, und ihm zum anderen über § 9 OWiG die Unternehmenseigenschaft zugerechnet werden kann. Als Beispiel wird in der Literatur die Vorstandssekretärin genannt, für deren Handlung der Betriebsleiter im Sinne von § 9 Abs. 2 Nr. 1 OWiG aufsichtspflichtig ist.[24] Daneben ist erforderlich, dass der Aufsichtspflichtige vorsätzlich oder fahrlässig seine Aufsichtspflicht gegenüber der zu beaufsichtigenden Person dadurch verletzt, dass er schuldhaft unterlassen hat, die kartellrechtswidrige Handlung zu unterbinden. Einen solchen Verstoß könnte beispielsweise eine unterbliebene Unterrichtung des Mitarbeiters über die wesentlichen Verbote des Kartellrechts darstellen.

3.5 Haftstrafe und Geldstrafe

Unternehmensmitarbeitern, die sich an Kartellrechtsverstößen beteiligen, drohen Haft und Geldstrafen. Paradebeispiel für die Strafverfolgung von Wettbewerbsverstößen sind die USA.

---

22 *Klusmann*, in: Wiedemann (Hrsg.), Handbuch des Kartellrechts, München 1999, § 55 Rn. 32, bezieht zum Beispiel auch „sachbearbeitende Schreibkräfte" in den Kreis dieser Personen ein, was in der Regel aber wohl den Begriff der „Eigenverantwortung" überdehnt und angesichts der Vermögensverhältnisse dieser Personen in der Regel für das Bundeskartellamt kaum interessant sein dürfte.

23 *Dreher*, ZWeR 2004, 75, 83, 91.

24 *Dreher*, ZWeR 2004, 75, 91.

So wurden dort zwischen 1997 und 2005 107 Personen zu Haftstrafen verurteilt, wobei gegen mehr als 40 Personen Strafen von einem Jahr oder länger verhängt wurden. Die durchschnittliche Gefängnisdauer betrug zwischen 2002 und 2005 19 Monate. Ein Viertel der Verurteilten waren Ausländer, darunter auch Deutsche. Die USA drängen auch mit internationalen Haftbefehlen über Interpol auf die Auslieferung beschuldigter Personen. So haben die USA von Großbritannien die Auslieferung von Ian Norris verlangt, eines britischen Staatsangehörigen, dem die USA vorwerfen, als Vorsitzender des Unternehmens Morgan Crucible Kartellverstöße in den USA begangen zu haben. Die britischen Behörden haben der Auslieferung stattgegeben. Die Berufung von Herrn Norris hat der High Court verworfen; das House of Lords wird das letzte Wort haben.[25] Für deutsche Staatsangehörige schließt zwar das Grundgesetz eine Auslieferung – zumindest in Länder außerhalb der Europäischen Union – aus.[26] Selbst ohne völkerrechtliches Auslieferungsabkommen kann ein deutscher Manager jedoch in die Lage geraten, Haft in den USA antreten zu müssen. Zum einen, wenn er sich dort zum Zeitpunkt der Verurteilung aufhält oder nach Verurteilung einreist. Zum anderen aber auch, falls ihn sein eigenes Unternehmen dazu bringt, sich zu stellen. Dies war im Jahr 2006 der Fall, als sieben koreanische Manager von Samsung ihre Teilnahme an einem Preiskartell gestanden und sich bereit erklärten, ihre Haft in den USA anzutreten.[27] Die strafrechtliche Verfolgung einzelner Personen wegen Verstößen gegen das Kartellrecht sind derzeit in Australien, Kanada, Irland, Israel, Japan, Korea, Großbritannien und den USA vorgesehen.[28]

In Deutschland drohen strafrechtliche Sanktionen demjenigen, der sich bei Ausschreibungen an wettbewerbswidrigen Absprachen beteiligt (§ 298 StGB). Oft ist nicht bekannt, dass diese Strafvorschrift nicht nur öffentliche, sondern auch private Ausschreibungen schützt. Auch der Straftatbestand des Betruges (§ 263 StGB) kann bei Kartellrechtsverstößen erfüllt sein. Wegen Ausschreibungsbetruges (Submissionsabsprache) wurden zum Beispiel zweieinhalb Jahre Haft sowie eine Geldstrafe gegen den Vertreter eines Bauunternehmens verhängt, der bei der Vergabe von Aufträgen der Flughafen München GmbH (Bau des Franz-Josef-Strauss-Flughafens) an Preisabsprachen beteiligt war.[29]

---

25 *Watson-Doig*, Crime and Competition. The Norris case and the future of competition enforcement, in: Competition Law Insight, 10. April 2006, S. 8 f.

26 Art. 16 Abs. 2 GG; das Auslieferungsverbot ist eingeschränkt bei einem Europäischen Haftbefehl.

27 *Watson-Doig*, Crime and Competition. The Norris case and the future of competition enforcement, in: Competition Law Insight, 10. April 2006, S. 8, 9.

28 *Rowley/Low/Wakil*, Increasing the Bite behind the Bark: Extradition in Antitrust Cases, Business Law International, 2007, S. 298.

29 BGH v. 11.7.2001 – 1 StR 576/00, NJW 2001, 3718.

3.6 Vorteilsabschöpfung

Durch die den Kartellbehörden eingeräumte Möglichkeit der Vorteilsabschöpfung kann sich der Ertrag und damit die Ausschüttung an die Gesellschafter mindern. Mindern können sich auch die Tantieme der Geschäftsleitung, soweit sie an den Ertrag geknüpft ist.

Hat ein Unternehmen durch einen schuldhaften Kartellrechtsvertstoß einen wirtschaftlichen Vorteil erlangt, kann die Kartellbehörde nach § 34 GWB die Abschöpfung dieses Vorteils anordnen und dem Unternehmen auferlegen, einen entsprechenden Geldbetrag zu zahlen. Auch die Verbesserung der Marktposition eines Unternehmens stellt einen solchen wirtschaftlichen Vorteil dar.[30] Die Vorteilsabschöpfung ist allerdings subsidiär zur Geldbuße, soweit diese den wirtschaftlichen Vorteil abschöpft, und zu zivilrechtlichen Schadensersatzleistungen.[31]

3.7 Schadensersatz

Während in Europa bislang das Bußgeldrisiko in der Regel der betragsmäßig größte Nachteil für Unternehmen darstellte, könnte im Einzelfall mittlerweile das Schadensersatzrisiko höher zu bewerten sein. Schadensersatzansprüche können die Höhe der Bußgelder um ein Vielfaches übertreffen. Bislang richten sich in Deutschland Schadensersatzklagen gegen Unternehmen; Ansprüche gegen Mitarbeiter, die durch ihr Handeln den Kartellverstoß begangen haben, sollen nach deutschem Recht aber nicht auszuschließen sein.[32] In den USA sind kartellrechtliche Schadensersatzansprüche bereits ein fester Bestandteil des Rechtsschutzsystems. *Treble damages* (dreifacher Schadensersatz), *class actions* (Sammelklagen) und *pre-trial discovery* (die Möglichkeit, von der Gegenseite und von unbeteiligten Dritten umfassende Informationen zu allen Tatsachen einzufordern, die für den behaupteten Klageanspruch relevant sein können) fördern und erleichtern dort die Geltendmachung von Schadensersatzansprüchen.

Aber auch in Europa ist mit einem starken Anstieg von Schadensersatzprozessen zu rechnen. Nach der Rechtsprechung des Europäischen Gerichthofes in der Sache Courage gegen Crehan[33] wäre das Kartellverbot nicht ausreichend wirkungsvoll, wenn nicht jedermann Schadensersatz für wettbewerbswidriges Verhalten erlangen könnte. Die Kommission hat sich auf die Fahnen geschrieben, die Ausübung des Rechts auf Erhebung von Schadenersatz wegen

30 *Bechtold*, in: Bechtold, GWB, 4. Aufl. 2006, § 34 Rn. 4.

31 § 34 Abs. 2 GWB.

32 So jedenfalls *Emmerich*, in: Immenga/Mestmäcker, GWB, 4. Aufl. 2007, § 33 Rn. 42.

33 Rs. C-453/99.

Wettbewerbsrechtsverletzungen (*private enforcement*) zu erleichtern. So hat sie ein Grünbuch zur privaten Kartellrechtsdurchsetzung veröffentlicht und will Anfang 2008 ein Weißbuch folgen lassen. Die Kommission stellt die Einführung von zweifachem Schadenersatz zur Diskussion. Ob dies die Mitgliedstaaten – sie, nicht die Kommission haben insoweit die Gesetzgebungskompetenz – übernehmen werden, ist derzeit offen. Die Kommission fördert die Kartellrechtsdurchsetzung durch Private derweil dadurch, dass sie in ihre Pressemitteilungen über die Verhängung von Geldbußen immer den Hinweis aufnimmt, betroffene Personen oder Unternehmen könnten vor den Gerichten der Mitgliedstaaten Klage auf Schadenersatz erheben und sich zum Beweis, dass das Verhalten tatsächlich stattgefunden hat und rechtswidrig war, auf die veröffentlichte Entscheidung stützen.

Erleichtert werden Klagen (sogenannte *follow-on* Klagen) auch dadurch, dass mittlerweile kein mitgliedstaatliches Gericht die rechtskräftige Feststellung eines Kartellrechtsverstoßes durch die Kartellbehörde eines anderen Mitgliedstaates in Frage stellen darf.[34]

Derzeit sind in Deutschland Klagen gegen das Zementkartell und in Österreich gegen das Aufzugherstellerkartell anhängig. In Großbritannien liegen mehrere Schadensersatzklagen vor dem Competition Appeal Tribunal.

3.8 Zivilrechtliche Unwirksamkeit

Vertragsbestimmungen, die gegen das Kartellrecht verstoßen, sind nichtig. Kaum jemand wird auf den Gedanken kommen, einen Kartellbruder auf Einhaltung einer rechtswidrigen Absprache zu verklagen. Abseits der Hardcore-Kartelle kann Compliance aber auch vermeiden, dass für sich genommen unproblematische Kooperationsverträge mit Wettbewerbern oder wichtige Vertriebsverträge ihren wirtschaftlichen Wert dadurch weitgehend einbüßen, dass zum Beispiel eine unzulässige Wettbewerbsbeschränkung den gesamten Vertrag oder wesentliche seiner Teile undurchsetzbar macht. Dies kann dazu führen, dass sich eine Partei von einem unliebsamen Vertrag lösen kann oder man zu neuen, ungünstigeren Konditionen neu verhandeln muss. Compliance bezweckt in diesem Zusammenhang also nicht in erster Linie den Schutz vor Geldbußen, Strafen und Schadensersatz, sondern sichert, dass die für das Unternehmen wesentlichen Verträge wirksam sind.

---

34 Art. 16 Abs. 1 VO 1/2003.

3.9 Wertverlust des Unternehmens

Kartellrechtliche Compliance sichert den Unternehmenswert. Unternehmenskäufer und Investoren stellen in der Regel bereits in der Due Diligence Fragen zu möglichen Kartellverstößen und beziehen dies in die Kalkulation des Kaufpreises, zuweilen sogar in die Kaufentscheidung selbst ein. So groß wird das Risiko einer Minderung des Unternehmenswertes durch Kartellbußen angesehen, dass sich die Garantie des Verkäufers, die Zielgesellschaft habe das Kartellrecht eingehalten, heute in jedem Mustervertrag findet. Aber nicht nur der Käufer will keine Leichen im Keller. Das Risiko eines schlechteren Ratings – insbesondere bei Wiederholungstätern – und eines sinkenden Börsenkurses sind nicht von der Hand zu weisen. So verloren die Aktien von Kühne & Nagel 5 % und von Panalpina 2,5 % an Wert nachdem bekannt wurde, dass europäische und amerikanische Wettbewerbsbehörden diese Speditionsunternehmen durchsucht hatten.[35]

Kunden und Lieferanten können – möglicherweise zu Recht – dem überführten Unternehmen bei künftigen Verhandlungen die Angemessenheit des Preises in Abrede stellen oder sich für die Vergangenheit schadlos halten wollen.

Ein Kartellverstoß wird in der Öffentlichkeit heutzutage nicht mehr als unbeachtliches Kavaliersdelikt gesehen; den genannten Speditionsunternehmen brachte ihr Erscheinen auf der Titelseite des Handelsblatts beachtliche Negativwerbung. Unternehmen, für die ein „sauberer Eindruck" in der Öffentlichkeit einen Wert darstellt, verlieren durch solche Schlagzeilen an Ansehen und müssen mit einigem PR-Aufwand gegensteuern.

3.10 Schadensersatz des Aufsichtsrats und des Vorstands an das Unternehmen

Gesellschaftsrechtliche Folgen eines Kartellverstoßes können insbesondere Aufsichtsrat und Vorstand in eine höchst diffizile Frontstellung gegeneinander bringen. Stellt das Bundeskartellamt fest, dass ein Vorstandsmitglied einen Verstoß selber begangen oder seine Aufsichtspflicht verletzt hat, wird damit nämlich möglicherweise auch feststehen, dass diese Person ihren Anstellungsvertrag verletzt hat. Damit wird die Gesellschaft zum Schadensersatz berechtigt (§ 93 Abs. 2 AktG).[36] Der Aufsichtsrat muss dann nach den Grundsätzen der ARAG/ Garmenbeck-Entscheidung des BGH[37] „die Geltendmachung der Ansprüche gegen den Vorstand zumindest ernsthaft prüfen".[38] Sieht der Aufsichtsrat pflichtwidrig von einer Geltend-

35 Handelsblatt vom 12. Oktober 2007, S. 1.

36 *Hauschka*, BB 2004, 1178 ff.

37 BGH v. 21.4.1997 – II ZR 175/95, BGHZ 235, 244 ff.

38 *Hauschka*, BB 2004, 1178 ff.

machung des Schadens gegen den Vorstand ab, macht er sich selber Schadensersatzpflichtig (§ 116 i.V.m. § 93 Abs. 2 AktG).[39]

3.11 Arbeitsrechtliche Folgen

Begeht ein Arbeitnehmer einen Kartellrechtsverstoß, kann dies eine arbeitsvertragliche Pflichtwidrigkeit begründen. Dann steht dem Unternehmen das gesamte arbeitsrechtliche Instrumentarium von Verwarnung, über Abmahnung, Versetzung bis zur Kündigung zur Verfügung. Das Arbeitsrecht richtet sich auch an Personen, die nicht von § 9 OWiG erfasst sind. In der Praxis sind diese arbeitsrechtlichen Fragen oft taktischen Aspekten untergeordnet, zum Beispiel der Überlegung, ob es sich das Unternehmen für eine effiziente Verteidigung leisten kann, auf die Kooperation dieses Arbeitnehmers zu verzichten.

3.12 Hindernis bei der Vergabe von Aufträgen und für die Karriere

Ein formal nebensächlicher Aspekt kann sich für den Einzelnen in der Praxis erheblich auswirken: Verhängt das Bundeskartellamt gegen eine natürliche Person ein Bußgeld, wird dies im Gewerbezentralregister vermerkt.[40] Diese Person gilt dann nicht mehr als „zuverlässig" im gewerberechtlichen Sinne. In vielen Fällen müssen Unternehmen ihre gewerberechtliche Zuverlässigkeit nachweisen, und das gilt nicht immer für das Unternehmen abstrakt, sondern zuweilen auch für bestimmte Personen im Unternehmen. Diese Zuverlässigkeit aber kann eine Voraussetzung sein z. B. in einem Vergabeverfahren. Eine kartellrechtliche Bestrafung kann diese Person und damit das Unternehmen von der Vergabe möglicherweise ausschließen. Bei Bußgeldern über 300 Euro wird die Eintragung im Gewerbezentralregister nach fünf Jahren getilgt.[41] Ein persönliches Problem kann sich zudem für Manager börsennotierter Unternehmen ergeben. Für notierte Aktiengesellschaften gelten neben Corporate Governance-Regeln die Vorschriften des Börsengesetzes, gemäß denen die Börsenaufsichtsbehörde darauf hinzuwirken hat, dass kartellrechtliche Vorschriften eingehalten werden.[42] Die BaFin kann daher zum Beispiel darauf hinwirken, dass am Kartell beteiligte Personen nicht in verantwortlicher Stellung in einem Unternehmen tätig sind oder werden.

---

39 BGH v. 21.4.1997 – II ZR 175/95, BGHZ 235, 244 ff.; *Hefermehl/Spindler*, in: MüKo/AktG, 2. Aufl. 2004, § 93 Rn. 24 ff.

40 § 149 Abs. 2 GewO.

41 § 153 Abs. 1 Nr. 2 GewO.

42 § 9 Börsengesetz.

3.13 Verfahrenskosten und Bindung von Mitarbeitern

Kartellverfahren können sich über mehrere Jahre erstrecken. Dies bedeutet nicht zu unterschätzende Belastungen für ein Unternehmen. So führt ein Bußgeldverfahren in der Regel dazu, dass sich Mitarbeiter für geraume Zeit nicht ihren eigentlichen Aufgaben widmen können, da sie eine erhebliche Menge an Informationen für das Verfahren zusammentragen müssen. Insbesondere für mittelständische Unternehmen mit einem verhältnismäßig kleinen Stamm nicht-operativer Mitarbeiter stellt dies eine große Belastung dar. Hinzu kommen die Kosten für externe Spezialisten, also Rechtsanwälte und zuweilen ökonomische Berater. Bei Verfahren in den USA oder anderen Staaten, in denen Kartellrecht Strafrecht ist, muss bedacht werden, dass während seiner Dauer die verdächtigten Manager längere Wartezeiten bei der Einreise einplanen müssen oder ohne vorherige Vereinbarung mit dem ermittelnden Staatsanwalt keine private oder geschäftliche Reise in die Vereinigten Staaten antreten können.

4. Kartellrechts-Compliance als Antwort

- Was kann Compliance leisten? –

4.1 Verstößen vorbeugen

Diese im vorherigen Abschnitt dargestellten Konsequenzen von Kartellrechtsverstößen für das Unternehmen, den Einzelnen und die Gesellschafter zeigen deutlich genug, dass es im ureignen Interesse aller Beteiligten liegt, Verstöße zu vermeiden. Kartellrechtliche Compliance muss daher zum Hauptzweck haben, durch organisatorische Maßnahmen Kartellrechtsverstößen vorzubeugen. Kein Verstoß, das bedeutet: kein Bußgeld, kein Schadensersatz usw.

4.2 Vorbereitung auf den Ernstfall

Compliance muss auch vorbereiten, wie das Unternehmen reagieren soll, wenn es einen Verstoß erkennt oder es von Kartellbehörden damit konfrontiert wird. Festzulegen ist zum

Beispiel, wie vorzugehen ist, wenn dem Unternehmen ein Fehlverhalten seiner Mitarbeiter bekannt wird: Wer berichtet an wen? Wer trifft letztlich die Entscheidung, ob eine Abstellung der Zuwiderhandlung ausreicht oder ob das Unternehmen darüber hinaus einen Kronzeugenantrag stellen sollte?

4.3 Aufsichtspflichtige enthaften

Kartellrechts-Compliance kann nach deutscher Rechtslage dazu dienen, die Unternehmensleitung vom Vorwurf einer Aufsichtspflichtverletzung zu entlasten. Aufsichtspflichtig gem. § 130 OWiG kann auch die Konzernmutter sein. Welche Anforderungen an die Geschäftsleiter und sonst verantwortlich Tätigen in den Obergesellschaften gestellt werden können, ist in der Literatur streitig.[43] Im Ergebnis wird eine konzernweite Compliance erforderlich sein, um das gesamte Management zu enthaften.

4.4 Geldbußen mindern?

Das Bundeskartellamt hat in der Vergangenheit Compliance-Programme bei der Festsetzug der Höhe des Bußgeldes nicht berücksichtigt.[44] Die Kommission berücksichtigte zwar in einigen früheren Entscheidungen Compliance-Maßnahmen als mildernde Umstände,[45] doch hat sie in letzter Zeit – etwa in ihrer Bußgeldentscheidung über das Aufzugskartell[46] – deutlich gemacht, dass sie solche Maßnahmen zukünftig nicht mehr berücksichtigen werde.[47] Das britische OFT hingegen lässt derzeit prüfen, welche Wirkungen Compliance-Programme haben. Abhängig vom Ausgang dieser Prüfung will das OFT solche Programme strafmindernd berücksichtigen. Dies scheint bereits der derzeitigen Praxis in Großbritannien zu entsprechen.

---

43 *Dreher*, Compliance Report, Heft 10, Oktober 2007, 3.

44 *Pampel*, BB 2007, 1636.

45 Kommission, 15. Juli 1992, ABl. L 233/27 ff. Rn. 24 – VIHO/Parker Pen.

46 Kommission, 21. Februar 2007.

47 Vgl. EuG v. 26.4.2007, verbn. Rs. T -109/02 u.a. – Bolloré; EuGH v. 28.6.2005, verb. Rs. C-189/02 P u.a. – Danks Rørindustri.

5. Bestandteile eines effektiven Compliance-Programms

- Wie muss Compliance organisiert sein? –

5.1 Maßstab für Effizienz

Konkrete Feststellungen dazu, welchen Inhalt Compliance-Programme haben müssen, finden sich weder in der Praxis des BKartA noch der deutschen Gerichte, der Kommission oder des Gerichtshofs. So beschränkt sich die Kommission eher auf allgemeine Feststellungen.[48] Entscheidend ist, was das Unternehmen erreichen und welchen Aufwand es dafür in Kauf nehmen will. In erster Linie wird Ziel die Haftungsvermeidung für das Unternehmen und das Führungspersonal sein. Dann ist die Aufsichtspflicht nach § 130 OWiG Ausgangspunkt für Vorschläge zum Inhalt und der Organisation der Kartellrechts-Compliance.[49] Erforderlich aber auch ausreichend ist nach dem BGH das „realistisch Zumutbare", „von starkem Misstrauen geprägte Aufsichtsmaßnahmen", die den Betriebsfrieden stören, können nicht verlangt werden.[50]

Das Compliance-Programm muss auf den Bedarf des jeweiligen Unternehmens zugeschnitten sein. Die britische Wettbewerbsbehörde OFT weist darauf hin, dass die Compliance-Maßnahmen von Unternehmen zu Unternehmen unterschiedlich sind und von vielen Faktoren, wie zum Beispiel von der Größe des Unternehmens und vom Feld seiner Betätigung abhängen.[51] Auch wird man prüfen müssen, in welchen Staaten das Unternehmen in Berührung mit kartellrechtswidrigen Handlungen kommen kann.

Während es für bestimmte, vor allem große Unternehmen ratsam ist, ein ausgefeiltes, das heißt aber auch teures und personell aufwendiges Compliance-Programm aufzusetzen, bieten sich für kleinere Unternehmen schlankere Lösungen an. So schreibt die OFT in einem Merkblatt, dass kleinere Unternehmen möglicherweise kein formelles Compliance-Programm benötigen, sie aber dennoch sicherstellen müssten, dass ihre Mitarbeiter sich bewusst seien, wie wichtig die Einhaltung der kartellrechtlichen Regelungen sei und welche Konsequenzen

48 *Pampel*, BB 2007, 1637, mit Verweis auf Kommission, 7. Dezember 1982, WuW/E EV 943, 946 – National Panasonic, in der die Kommission sagt, es habe sich um ein „umfassendes, praktikables, detailliertes und sorgfältig abgewogenes Programm" gehandelt.

49 *Pampel*, BB 2007, 1637; *Dreher*, ZWeR 2004, 75, 93 f.

50 BGH v. 11.3.1986 – KRB 7/85, WuW/E BGH 2262, 2264.

51 http://www.oft.gov.uk/shared_oft/business_leaflets/ca98_mini_guides/oft424.pdf; siehe auch *Janssen/Wüstenfeld*, Compliance Report, Heft 10, Oktober 2007, 5 ff.

sich aus einem Verstoß gegen die Wettbewerbsvorschriften ergeben können.[52] Die Einsetzung eines Compliance-Beauftragten mag bereits einen wesentlichen Schritt zur Haftungsvermeidung darstellen.[53]

5.2 Kartellrechts-Compliance ist Chefsache

Nur wenn die Unternehmensleitung für Compliance eintritt, lohnt sich der Aufwand. Sie muss ihren Mitarbeitern deutlich zu verstehen geben, dass sie der Compliance einen angemessenen Stellenwert im Unternehmen gibt. Dies zeigt sich zum Beispiel dadurch, dass die wesentlichen Maßnahmen von der Unternehmensleitung angeordnet und kommuniziert werden. Delegiert sie diese Aufgaben zum Beispiel auf einen Compliance Officer, muss sichtbar werden, dass sie ihn stützt.

Dass die Mitglieder der Unternehmensleitung persönlich gefordert sind, ergibt sich aus den Urteilen zur Delegation von Aufsichtspflichten. Auch wenn danach die konkrete Durchführung von Instruktion, präventiver Kontrolle und repressiver Sanktionierung durch die Unternehmensleiter delegierbar ist, bleibt dem „Betriebsinhaber" im Sinne von § 130 OWiG beziehungsweise den bei juristischen Personen nach § 9 Abs. 1 OWiG verantwortlichen gesetzlichen Vertretern eine eigene „Oberaufsicht".[54]

5.3 Risikoanalyse

Im Vorfeld der Etablierung eines Compliance-Programms muss analysiert werden, in welchem Maße für das Unternehmen das Risiko von Kartellrechtsverstößen besteht. Bei einem erhöhten Risiko drängen sich verständlicherweise umfassendere Maßnahmen auf. Für die Analyse, ob und für welche Kartellrechtsverstöße das eigene Unternehmen anfällig ist, mögen folgende Fragen nützlich sein:[55]

- Ist das Unternehmen bereits einmal bebußt oder durchsucht worden?
- Sind Wettbewerber durchsucht oder bebußt worden?

---

52 Vgl. http://www.oft.gov.uk/shared_oft/business_leaflets/ca98_mini_guides/oft424.pdf

53 *Hauschka*, BB 2004, 1178 ff.

54 *Dreher*, ZWeR 2004, 75, 94 f.; vgl. auch Kapitel 1, 40.

55 Vgl. http://www.oft.gov.uk/shared_oft/business_leaflets/ca98_mini_guides/oft424.pdf¸ *Kapp*, Kartellrecht in der Unternehmenspraxis, 2005, 228.

- Gab es auf anderen Marktstufen (Lieferanten, Abnehmer) kartellrechtliche Ermittlungen?
- Hat mein Unternehmen eine marktbeherrschende Stellung auf einem der Märkte, auf dem es tätig ist? Nur dann ist ein Verstoß gegen das Missbrauchsverbot denkbar.
- Besteht für Mitarbeiter in den Bereichen Verkauf, Vertrieb, Marketing und Einkauf die Möglichkeit, ohne Kenntnis der Geschäftsführung mit Wettbewerbern wettbewerbswidrige Vereinbarungen zu treffen, insbesondere Preiserhöhungen zu kommunizieren, Gebiete und Kundenkreise abzusprechen?
- Haben Angestellte, haben Führungskräfte regelmäßigen Kontakt mit Wettbewerbern? Auf welchen Foren trifft man sich (zum Beispiel in Verbänden)? Welche Informationen werden dort ausgetauscht?
- Ist die Branche durch einen starken Wettbewerb gekennzeichnet oder sind die Verhältnisse seit längerem unverändert?
- Sind viele oder wenige Wettbewerber in der Branche tätig?
- Wissen die Wettbewerber viel oder wenig über die geschäftlichen Tätigkeiten des jeweils anderen?
- Gibt es gemeinsame Marktinformationssysteme?
- Welche Kooperationen mit Wettbewerbern bestehen?

Die Risikoanalyse ist auch insoweit von Bedeutung, als unter bestimmten Voraussetzungen höhere Anforderungen an die Kartellrechts-Compliance zu stellen sind. Zum Beispiel dann, wenn konkrete Anhaltspunkte für den Verdacht bestehen, das sich Unternehmensmitarbeiter an Kartellrechtsverstößen beteiligen oder in einer bestimmten Branche Submissionsabsprachen häufig vorkommen. Dann können z. B. häufigere Schulungen, Einzelgespräche oder gezielte Überwachung erforderlich werden.[56] Zur Risikoabschätzung gehört auch die Frage, ob Unternehmensmitarbeiter, die mit Aufgaben betraut werden sollen, die „zu kartellrechtsrelevantem Handeln führen", sorgfältig ausgewählt werden.[57]

5.4 Instruktion der Mitarbeiter

Ziel der Instruktion ist es, Kenntnisse über die kartellrechtlichen Verbote und ihren Zweck zu vermitteln. Die Hinweise müssen auf die Branche und die jeweilige Tätigkeit zugeschnitten sein. Nichtjuristen müssen sie verstehen können. Gerade die haftungsträchtigen Kernbeschränkungen lassen sich leicht erklären. Die Wertungen werden in der Regel von allen – zumindest abstrakt – geteilt. Typische Beispiele müssen gebracht und konkrete Handlungs-

56 *Dreher*, ZWeR 2004, 75, 95.

57 KG v. 25.7.1980 – Kart 26/79, WuW/E OLG 2330, 2332 – Revisionsabteilung.

anweisungen gegeben werden. Wer etwa an Treffen, wo wettbewerbswidrige Inhalte besprochen werden, teilnimmt, muss sich „offen vom Inhalt der Sitzungen distanzier[en]“[58] oder Umstände nachweisen, „aus denen sich eindeutig eine fehlende wettbewerbswidrige Einstellung bei der Teilnahme an Sitzungen ergibt“.[59.] Grenzfälle – oder Unklarheiten in der Rechtslage – müssen die Mitarbeiter nicht selbst entscheiden. Es geht nicht darum, Kartellrechtsspezialisten auszubilden oder unternehmerische Spielräume einzuengen. Im Kern geht es um eine Sensibilisierung der Mitarbeiter.

Für subjektive Unsicherheiten und objektive Zweifelsfälle muss organisatorisch gesichert sein, dass der betroffene Mitarbeiter sich an einen Zuständigen wenden kann. Allgemeine Hinweise nach dem Motto, bei Problemen die Rechtsabteilung einzuschalten oder das Kartellrecht zu beachten, sieht die Rechsprechung als unzureichend für eine Enthaftung nach § 130 OWiG an.[60]

Das einfachste Mittel zur Durchführung von Instruktionen sind Mitarbeiterschulungen. Je nach Größe des Unternehmens und des betroffenen Personenkreises können sie als Präsenz-Schulungen oder elektronisch durchgeführt werden. Präsenz-Schulungen sind in fast jeder Hinsicht vorzugswürdig. Sie erlauben eine Interaktion und gewähren auch der Unternehmensleitung zuweilen einen überraschenden Einblick in die Gepflogenheiten ihrer Mitarbeiter. Die Mitarbeiter sollten im Vorfeld von Schulungen um ihre Fragen und Anmerkungen gebeten werden. Schriftliche Kartellrechts-Richtlinien können dies unterstützen, wobei man sich über die Lektüre von „Handbüchern“, insbesondere durch Nicht-Juristen keine Illusionen machen sollte. Kurz gefasste Richtlinien helfen jedoch den Mitarbeitern, nach eigenem Belieben nachzulesen, und der Unternehmensleitung, sich auf sie zu berufen.[61] Die wesentlichen Informationen passen oft auf ein personalausweisgroßes Format.[62] Die Teilnahme an einer Schulung und gegebenenfalls den Empfang und das Lesen der Richtlinien sollten die Mitarbeiter schriftlich bestätigen. Je nach Unternehmen, Branche und Personalfluktuation sollten Mitarbeiter in regelmäßigen Abständen geschult werden.

5.5 Motivation

Will die Unternehmensleitung eine Compliance-Kultur in ihrem Unternehmen durchsetzen, muss sie mit gutem Beispiel vorangehen. Dazu kann auch gehören, die Vergütungsanreize zu überdenken und neu festzusetzen. Eine einfache Maßnahme ist die Formulierung einer Compliance-Policy, an die sich alle im Unternehmen halten sollen.

---

58 EuG v. 14. 5. 1988 – Rs T – 334/94, Slg. 1998 II, 1439 – Sarriò.

59 EuGH v. 8.7.1999 – Rs C – 199/92 P, Slg. 1999 I, 4287 – Hüls gegen Kommission.

60 KG v. 25.7.1980 – Kart 26/79, WuW/E OLG 2230, 2232 – Revisonsabteilung.

61 Vgl. *Dreher*, ZWeR 2004, 75, 98.

62 Siehe zum Beispiel die Do´s & Don’ts im Kartellrecht auf www.luther-lawfirm.com.

5.6 Kontrolle

Bestandteil einer effektiven Katellrechts-Compliance können auch regelmäßige Überwachungsmaßnahmen sein, um sicherzustellen, dass keine Kartellrechtsverstöße begangen werden. Hinzuweisen ist dabei zum einen auf die Auswahl eines Ansprechpartners für Zweifelsfragen, etwa in der Rechtsabteilung des Unternehmens. Dabei ist es wichtig, den Aufgaben- und Verantwortungsbereich dieses Ansprechpartners genau abzugrenzen, wobei die Oberaufsicht nach der Rechsprechung immer bei der Geschäftsleitung bleibt.[63]

Zum anderen ist auf den Punkt „stichprobenhafte Prüfungen" hinzuweisen, den die Rechtsprechung bei verschiedenen Gelegenheiten behandelt hat. So stellte der BGH etwa fest: „Das Kammergericht geht zur Recht davon aus, daß der Betroffene die Revisionsabteilung so hätte organisieren müssen, daß sie in der Lage gewesen wäre, in allen Verkaufsbüros wenigstens stichprobenartige überraschende Prüfungen durchzuführen. Derartige Prüfungen sind erforderlich und regelmäßig auch geeignet, vorsätzliche Zuwiderhandlungen gegen gesetzliche Vorschriften und Anweisungen der Betriebsleitung zu verhindern, denn sie halten den Betriebsangehörigen vor Augen, daß solche Verstöße entdeckt und gegebenenfalls geahndet werden können. Für weitergehende Kontrollen musste der Betroffene im vorliegenden Fall nicht sorgen."[64]

5.7 Zuwiderhandlung abstellen

Stellt die Compliance einen Verstoß fest, muss das Unternehmen sehr schnell die Schwere und das Risiko der Entdeckung bewerten. Entschließt sich das Unternehmen daraufhin, die Zuwiderhandlung abzustellen, muss es damit rechnen, dass die anderen beteiligten Unternehmen unruhig werden und eventuell selbst einen Antrag auf Kronzeugenbehandlung stellen. Dann beginnt ein Wettrennen zu den Kartellbehörden, denn für die Gewährung des Kronzeugenstatus gilt das Windhundprinzip.

5.8 Dokumentation

Die Instruktion und die Überwachungsmaßnahmen sollten dokumentiert werden. Dies ermöglicht eine frühzeitige und sachgerechte Reaktion der Unternehmensleitung. Werden zum

---

63 Vgl. *Dreher*, ZWeR 2004, 75, 99.

64 BGH, Beschl. v. 24.3.1981 – KRB 4/80, wistra 1982, 34.

Beispiel abgelehnte Avancen von Wettbewerbern dokumentiert, kann man sich bei Ermittlungen durch die Kartellbehörden leicht entlasten und somit den Aufwand des Verfahrens reduzieren.

Individuell zu beantworten ist die Frage, was genau und in welchem Umfang das Unternehmen dokumentieren soll. Dies gilt besonders für den Fall, dass ein Unternehmen bei der Kontrolle seiner Mitarbeiter Verstöße aufdeckt. Selbst wenn das Verhalten sofort abgestellt wird, nimmt die Dokumentation, sollte sie bei späteren Ermittlungen in die Hände der Wettbewerbsbehörden gelangen, dem Unternehmen wesentliche Verteidigungsmöglichkeiten.

Das Problem stellt sich mit aller Schärfe, da nach derzeitiger Rechtslage solche Dokumente beim Compliance Offier oder beim Syndikus des Unternehmens nicht sicher vor Beschlagnahme sind: Nach der – gerade im Urteil AKZO[65] bekräftigten – Rechtsprechung der europäischen Gerichte erfasst das Legal Privilege nicht die Korrespondenz mit einem Syndikusanwalt. Einzig die Korrespondenz mit unabhängigen unternehmensexternen Anwälten ist geschützt. Die deutschen Gerichte beantworten die Frage, ob die Unterlagen eines Syndikusanwalts beschlagnahmefrei sind, uneinheitlich.[66] Sicher beschlagnahmefrei ist nach europäischem und deutschem Recht Anwaltskorrespondenz (Korrespondenz an Anwälte und von Anwälten) im Rahmen eines laufenden Straf- und Ordnungswidrigkeitenverfahrens. Sicher beschlagnahmefrei sind sowohl nach europäischem als auch nach deutschem Recht die Unterlagen, die sich im alleinigen Gewahrsam eines externen Rechtsanwalts befinden. Insbesondere Compliance Officer, die kartellrechtlich bedenkliches Handeln von Mitarbeitern identifizieren und dokumentieren, müssen sich genau darüber informieren, wie sie im Sinne des Unternehmens die Beschlagnahmefreiheit ihrer Notizen und Berichte sichern.

5.9 Sanktion

Ebenfalls Bestandteil einer effektiven Kartellrechts-Compliance ist eine Sanktionierung von Kartellrechtsverstößen.[67] Denn nur so kann ein Unternehmen glaubwürdig zeigen, dass es einen Kartellrechtsverstoß nicht augenzwinkernd als Kavaliersdelikt durchgehen lässt. Eine Sanktionierung von Kartellrechtsverstößen erhöht insbesondere die Aufmerksamkeit und schreckt ab.

Treten Kartellrechtsverstöße trotz Compliance-Maßnahmen ein, kann es angezeigt sein, arbeitsrechtliche Konsequenzen gegen den betroffenen Mitarbeiter einzuleiten. Allerdings kann der Rechtsprechung keine Verpflichtung entnommen werden, Unternehmensmitarbeitern ohne weiteren Anlass für den Fall eines Kartellrechtsverstoßes arbeitsrechtliche Sanktionen anzudrohen.[68]

---

65 EuG v. 17.9.2007, verb. Rs. T-125/03 und T – 253/03 – Akzo Nobel gegen Kommission.

66 *Schumacher*, Compliance Report, Heft 10, Oktober 2007, 12 f.

67 *Dreher*, ZWeR 2004, 75, 100.

68 BGH, v. 24.3.1981 – KRB 4/80, wistra 1982, 34.

5.10 Krisenmanagement

Keine organisatorische Vorkehrung kann Verstöße ausschließen. Eine gute Compliance-Organisation entdeckt unvorhergesehene Regelwidrigkeiten jedoch früher oder später. Für diesen Fall muss die Unternehmensleitung sich zumindest ihre wesentlichen Reaktionen vorab überlegen. Wie will man bei einem Verstoß reagieren? Man kann sicherlich keine allgemein richtige Antwort geben. Aber zumindest sollte klar sein,

- dass ein solcher Fall höchste Priorität genießt,
- wer in der Geschäftsleitung sich um die Vorbereitung einer Entscheidung kümmert und
- was man dokumentiert.

Zum Standard gehört auch ein Notfallplan für den Fall, dass Kartellbehörden das Unternehmen durchsuchen.[69]

[69] *Kapp*, Kartellbehörde durchsucht Geschäftsräume – Was ist zu beachten?, Compliance Report, Heft 10, Oktober 2007, 3-5.

Compliance in der arbeitsrechtlichen Praxis

Katrin Süßbrich

Zusammenfassung

Auch wenn der Ursprung des Themenfeldes Compliance sicherlich im Bereich der großen, an den US-amerikanischen Börsen notierten Unternehmen der Kredit- und Finanzwirtschaft zu suchen ist, hat Compliance längst Einzug in deutsche Unternehmen aller Branchen erhalten. Hierzu hat nicht zuletzt das am 18. August 2006 in Kraft getretene Allgemeine Gleichbehandlungsgesetz (*AGG*) beigetragen, das in § 12 Abs. 1 AGG den Arbeitgeber verpflichtet, die erforderlichen Maßnahmen zum Schutz vor Benachteiligungen im Sinne des Gesetzes zu treffen, wobei ausdrücklich auch vorbeugende Maßnahmen umfasst sind. Auch wenn es – zumindest bisher – glücklicherweise nicht zu der vielfach befürchteten Flut von Schadensersatz- und Entschädigungsklagen nach dem AGG gekommen ist und vor dem Hintergrund der deutschen Rechtsprechungspraxis insbesondere Entschädigungssummen nach amerikanischem oder britischem „Vorbild" ausbleiben dürften,[1] wurde bis zum Inkrafttreten des AGG häufig übersehen, dass insbesondere die Einhaltung arbeitsrechtlicher Gesetze wichtiger Bestandteil der Compliance ist. Denn bei einer Verletzung arbeitsrechtlicher Vorschriften drohen empfindliche (materielle und immaterielle) Schäden sowohl für das Unternehmen als auch für die persönlich haftenden Organe. Vorbeugende Organisationsmaßnahmen sind damit für den Arbeitgeber unerlässlich.

Vor diesem Hintergrund sollen deshalb zunächst die haftungsträchtigsten arbeitsrechtlichen Vorschriften hervorgehoben werden. Im Anschluss daran werden die Möglichkeiten zur verbindlichen Einführung wirksamer Compliance-Systeme im Unternehmen dargestellt.

---

1 Die Deutsche Bank wurde 2006 von einem Londoner Gericht zur Zahlung von Schadenersatz in Höhe von 1,2 Mio € an ein „Mobbingopfer" verurteilt.

1. Arbeitsrechtliche Vorschriften mit Haftungsrisiko

1.1 „Klassischer“ Arbeitsschutz

Dem Arbeitgeber obliegen in Bezug auf seine Arbeitnehmer unabdingbare Fürsorgepflichten. Hierzu zählt insbesondere die Verpflichtung, die Arbeitnehmer an ihrem Arbeitsplatz und bei der Arbeitsleistung vor gesundheitlichen Gefahren zu schützen (§§ 618, 619 BGB, 62 HGB). Eine Konkretisierung dieser aus dem Arbeitsverhältnis selbst erwachsenden Fürsorgepflicht erfolgt inzwischen durch eine Vielzahl von öffentlich-rechtlichen Schutzvorschriften.

Die Beachtung der Arbeitsschutzbestimmungen und die damit verbundene Verhütung von Arbeitsunfällen und Betriebskrankheiten sind deshalb an erster Stelle zu nennen, da Pflichtverletzungen des Arbeitgebers in diesem Bereich zu Personen- und Sachschäden in erheblichem Umfang führen können. Verletzt der Arbeitgeber dabei vorsätzlich oder grob fahrlässig seine Pflichten, kann die Berufsgenossenschaft den Arbeitgeber z. B. in die Regresspflicht nehmen (§ 110 Abs. 1 SGB VII).

Zu den wichtigsten gesetzlichen Arbeitsschutzvorschriften eines der ältesten Arbeitsrechtsthemen schlechthin zählt insbesondere das Arbeitsschutzgesetz (ArbSchG). Des Weiteren sind neben den Beschäftigungsverboten für bestimmte Personengruppen (z. B. im Mutterschutzgesetz, Jugendarbeitsschutzgesetz und in der Kinderarbeitsschutzverordnung) das Arbeitssicherheitsgesetz (ASiG) mit seiner Verpflichtung zur Bestellung von Betriebsärzten und Fachkräften für Arbeitssicherheit[2] sowie die von den Berufsgenossenschaften erlassenen Arbeitsschutz- und Unfallverhütungsvorschriften zu beachten. Im Einzelfall sind daneben besondere Vorschriften, z. B. die Bildschirmarbeitsverordnung für Bildschirmarbeitsplätze, zu berücksichtigen, deren Verletzung mit Bußgeld sanktioniert ist.

In den Bereich des Arbeitsschutzes fällt schließlich auch das Arbeitszeitgesetz (ArbZG). § 3 ArbZG sieht vor, dass die werktägliche Arbeitszeit acht Stunden nicht überschreiten darf. Die Arbeitszeit kann indes auf bis zu zehn Stunden verlängert werden, wenn innerhalb von sechs Kalendermonaten oder 24 Wochen im Durchschnitt wieder acht Stunden erreicht werden. Daneben sind die gesetzlich vorgegebenen Pausen (30 bis 45 Minuten bei einer Arbeitszeit über sechs Stunden) und Ruhezeiten (grundsätzlich 11 Stunden) zu beachten. Verletzungen der arbeitszeitrechtlichen Vorschriften werden als Ordnungswidrigkeiten mit einer Geldbuße von bis zu 15.000,00 € geahndet, wobei diese Geldbuße für jeden einzelnen Verstoß – ggf. auch wiederholt – verhängt werden kann. Im Falle einer beharrlichen Wiederholung oder einer Gefährdung der Gesundheit oder Arbeitskraft eines Arbeitnehmers liegt sogar eine Straftat vor (§ 23 ArbZG).

---

[2] Diese Pflicht trifft gemäß §§ 1, 2, 5 ASiG nur Unternehmen, bei denen dies u. a. aufgrund ihrer Betriebsart, der Zahl der Beschäftigten, Zusammensetzung der Arbeitnehmerschaft und Betriebsorganisation erforderlich ist. Die konkretisierende behördliche Anordnung ergeht auf der Grundlage des § 12 ASiG.

1.2 Sozialversicherung

Bedeutende finanzielle Haftungsrisiken für den Arbeitgeber ergeben sich insbesondere im Bereich der Sozialversicherung. Schuldner der Sozialversicherungsabgaben (Beiträge zur gesetzlichen Kranken-, Pflege-, Renten- und Arbeitslosenversicherung) ist nämlich alleine der Arbeitgeber, wobei sich die Schuldnerstellung ausdrücklich auf den Gesamtsozialversicherungsbeitrag und damit gerade nicht nur auf den Arbeitgeberanteil erstreckt (§ 28 e Abs. 1 S. 1 SGB IV). Der Arbeitgeber hat mithin unbedingt die ordnungsgemäße Abführung aller Sozialversicherungsabgaben sicherzustellen. Hinzu kommt, dass dem Arbeitgeber zwar gegen den Arbeitnehmer ein Ausgleichsanspruch in Höhe des auf den Arbeitnehmer entfallenden Beitragsteils zusteht. Dieser Anspruch kann indes nur durch Abzug vom Arbeitsentgelt und insbesondere nur bei den nächsten drei Lohn- oder Gehaltszahlungen, also für maximal drei Monate, durchgesetzt werden (§ 28 g S. 3 SGB IV).

Die nicht rechtzeitige oder nicht vollständige Erfüllung dieser Pflicht stellt § 266 a des Strafgesetzbuchs (StGB) darüber hinaus unter den Straftatbestand des sog. „Sozialversicherungsbetrugs“. Als „Täter“ sieht das StGB insoweit den Arbeitgeber vor, persönlich sind damit aber die Organe der Gesellschaften in der Pflicht (§ 14 Abs. 1 StGB).[3]

In diesem Zusammenhang spielt auch die Problematik der Scheinselbständigkeit eine entscheidende Rolle. Denn der Arbeitgeber muss bei der für den Einzug der Sozialversicherungsabgaben zuständigen Stelle jeden bei ihm Beschäftigten melden. Beschäftigt i.d.S. ist indes nur derjenige, der nichtselbständige Arbeit verrichtet (§ 7 Abs. 1 SGB IV). Die Abgrenzung zwischen selbständiger und nichtselbständiger Arbeit ist in vielen Fällen schwierig und bedarf einer umfassenden Abwägung aller Umstände des Einzelfalls. In Zweifelsfällen sollte das Statusfeststellungsverfahren bei der Deutschen Rentenversicherung Bund gemäß § 7 a SGB IV durchgeführt werden. Denn Scheinselbständige, die nach außen wie selbständig tätige Unternehmer auftreten, faktisch jedoch weisungsgebunden sind, gelten sozialversicherungsrechtlich als Beschäftigte.[4] Liegt eine Scheinselbständigkeit vor, muss der Arbeitgeber jedoch mit Wirkung für die Vergangenheit – ggf. bis zum Ablauf der Verjährungsfrist von vier Jahren (§ 25 SGB IV) – die Gesamtsozialversicherungsbeiträge nachzahlen. Ein Erstattungsanspruch gegen den Arbeitnehmer besteht auch insoweit nur für die letzten drei Monate. Hält man sich vor Augen, dass die Gesamtsozialversicherungsabgaben zur Zeit ca. 40 % der dem Arbeitnehmer gewährten Vergütung betragen und alleine durch die Beitragsbemessungsgrenze gedeckelt sind, wird deutlich, welches (finanzielle) Haftungsrisiko sich hier verbirgt. Daneben tritt auch insoweit wieder die strafrechtliche Verantwortung gemäß § 266 a StGB.

---

3 Zur Verantwortung eines GmbH-Geschäftsführers in der finanziellen Krise der Gesellschaft etwa: BGH v. 9.1.2001 – VI ZR 407/99, NJW 2001, S. 969 ff.

4 Vgl. auch *Pelz/Steffek*, in: Hauschka (Hrsg.), Corporate Compliance, München 2007, § 19 D Rn. 33 m.w.N.

1.3 AGG

Das AGG dürfte in den vergangenen 1 ½ Jahren mit Abstand das am häufigsten diskutierte Compliance-Thema in den Unternehmen gewesen sein. Eine Vielzahl von Unternehmen sind in der Zwischenzeit der in § 12 Abs. 1 und Abs. 2 AGG normierten Pflicht des Arbeitgebers nachgekommen, (vorbeugende) Maßnahmen zum Schutz der Arbeitnehmer vor Diskriminierungen zu treffen und haben ihre Mitarbeiter durch Personalschulungen oder e-learning Angebote zum AGG geschult. Darüber hinaus sind sog. „codes of conduct" (Ethikrichtlinien oder Verhaltenskodizes) und „Whistleblower-Hotlines" zumindest in großen Unternehmen vielfach schon gängige Praxis.[5]

Das AGG schützt vor Diskriminierungen (das Gesetz verwendet insoweit den Begriff der Benachteiligung) aus Gründen der Rasse oder ethnischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität. Dabei sieht das Gesetz fünf Formen der Benachteiligung vor. Die unmittelbare und die mittelbare Benachteiligung, die Belästigung und die sexuelle Belästigung sowie die Anweisung zur Benachteiligung. Nicht nur inhaltlich bietet das AGG mithin einen umfassenden Schutz für die Arbeitnehmer. Vielmehr ist auch der sachliche und persönliche Anwendungsbereich des arbeitsrechtlichen Teils des AGG weit gefasst. So sind insbesondere Diskriminierungen in Bezug auf Arbeitsbedingungen einschließlich Arbeitsentgelt und Entlassungsbedingungen, insbesondere in individual- und kollektivrechtlichen Vereinbarungen sowie Maßnahmen bei der Durchführung und Beendigung eines Beschäftigungsverhältnisses unzulässig (§ 2 Abs. 1 Nr. 2 AGG). In den persönlichen Schutzbereich des AGG fallen daneben nicht nur alle bereits beschäftigten Arbeitnehmerinnen und Arbeitnehmer, sondern insbesondere auch alle Bewerberinnen und Bewerber sowie die Auszubildenden. Organmitglieder sind hingegen „nur" geschützt, soweit es um die Bedingungen für den Zugang zur Erwerbstätigkeit sowie den beruflichen Aufstieg geht.

Liegt eine Benachteiligung im vorgenannten Sinne vor, haftet der Arbeitgeber gemäß § 15 AGG bei einem tatsächlich bezifferbaren Schaden auf Schadenersatz in unbegrenzter Höhe; wegen eines Schadens, der nicht Vermögensschaden ist (immaterieller Schaden; sog. „Schmerzensgeld"), muss der Arbeitgeber eine Entschädigung in Geld leisten. Diese ist nur für den Fall der Nichteinstellung eines Bewerbers auf drei Monatsgehälter beschränkt, wenn der Bewerber auch bei benachteiligungsfreier Auswahl nicht eingestellt worden wäre. Im Übrigen ist die Entschädigung unbegrenzt. Auch wenn – worauf eingangs bereits hingewiesen wurde – nicht zu erwarten ist, dass die deutschen Gerichte (z. B. bei einer Belästigung im Sinne des AGG) Entschädigungssummen nach amerikanischem oder britischem „Vorbild" zusprechen werden, liegt hierin doch ein beträchtliches Risiko für den Arbeitgeber. Dies gilt nicht zuletzt deshalb, weil das Gesetz in § 22 AGG eine wesentliche Beweiserleichterung für den jeweiligen Kläger vorsieht. Im ersten Schritt genügt für den Kläger nämlich bereits der

---

5 Zu der Frage, ob der Arbeitgeber durch die Implementierung von Ethikrichtlinien bereits seiner Pflicht aus § 12 Abs. 1 AGG genügt, vgl. zutreffend kritisch *Schneider/Sittard*, NZA 2007, 654 ff.

Beweis bloßer Indizien, die eine Benachteiligung wegen eines Diskriminierungsmerkmals vermuten lassen, um den Arbeitgeber in Bedrängnis zu bringen. Dieser muss im Anschluss beweisen, dass die Diskriminierung tatsächlich nicht stattgefunden hat.

1.4 Arbeitnehmerüberlassung

Der Arbeitnehmerüberlassung kommt insbesondere in großen Konzernen immer mehr Bedeutung zu. Während die vorübergehende Arbeitnehmerüberlassung zwischen Konzernunternehmen erlaubnisfrei möglich ist, bedarf die gewerbsmäßige Arbeitnehmerüberlassung an Dritte einer behördlichen Erlaubnis im Sinne des Arbeitnehmerüberlassungsgesetzes (AÜG). Hiernach liegt Arbeitnehmerüberlassung vor, wenn ein Arbeitgeber (Verleiher) bei ihm beschäftigte Arbeitnehmer (Leiharbeitnehmer) gewerbsmäßig an einen Dritten (Entleiher) zur Arbeitsleistung überlässt und dieser Arbeitnehmer in dem Betrieb des Entleihers nach dessen Vorstellung und unter dessen Weisung tätig wird. Gewerbsmäßig ist die Arbeitnehmerüberlassung dann, wenn sie nicht nur gelegentlich erfolgt, sondern auf gewisse Dauer angelegt und auf Erzielung wirtschaftlicher Vorteile gerichtet ist.

Folge einer ohne die hierfür erforderliche Erlaubnis erfolgenden Arbeitnehmerüberlassung ist nicht nur die Begründung eines Arbeitsverhältnisses kraft Gesetzes zwischen Entleiher und Leiharbeitnehmer: der Entleiher ist damit für die Lohnzahlung nach den in seinem Betrieb geltenden Bestimmungen sowie für die Abführung der Sozialversicherungsbeiträge verantwortlich; daneben haftet er wie jeder andere Arbeitgeber auch für die Lohnsteuer (§ 42 d Abs. 7 EStG). Darüber hinaus ist ein Verstoß gegen das AÜG auch als Ordnungswidrigkeit mit einem Bußgeld belegt. Das Bußgeld beträgt bis zu 25.000,00 € (§ 16 Abs. 2 i.V.m. § 16 Abs. 1 Nr. 1 AÜG).

In der Praxis werden vor dem Hintergrund der Erlaubnispflicht sowie des mit dem AÜG verbundenen sog. „Equal-pay-Gebots“ (Pflicht zur Vergütung der Leiharbeitnehmer entsprechend den Bedingungen im Entleiherbetrieb) vielfach Werk- oder Dienstverträge für den Einsatz betriebsfremder Arbeitnehmer geschlossen. In den überwiegenden Fällen werden die Arbeitnehmer indes in die Betriebsorganisation sowie unter die Weisungen des „Auftragnehmers“ eingegliedert. Vor dem Hintergrund der vorstehenden Rechtsfolgen, insbesondere der Fiktion eines Arbeitsverhältnisses, ist vor dem Einsatz betriebsfremder Arbeitnehmer stets sorgfältig zu prüfen, ob nicht eine erlaubnispflichtige Arbeitnehmerüberlassung vorliegt.

1.5 Ausländerbeschäftigung

Die Beschäftigung eines Ausländers, der nicht (mehr) im Besitz eines gültigen Aufenthaltstitels ist, ist nach den Regelungen des Aufenthaltsgesetzes sowie den Bestimmungen des Schwarzarbeitergesetzes mit Bußgeld von bis zu 500.000,00 € (§§ 98 Abs. 2a i.V.m. 4 Abs. 3 S. 2 AufenthG) bzw. von bis zu 300.000,00 € (§ 8 Abs. 1 Nr. 2, Abs. 3 SchwarzArbG bewehrt. Nach § 11 SchwarzArbG kommt sogar eine Freiheitsstrafe in Betracht. Daneben haftet der Arbeitgeber für die Kosten der Abschiebung (§ 66 Abs. 4 AufenthG). Zu diesen Kosten gehören neben den erforderlichen Beförderungskosten auch die entstandenen Verwaltungskosten.

1.6 Datenschutz

Auch die Beachtung datenschutzrechtlicher Vorgaben ist unerlässlich. Mit Hilfe von EDV-Anlagen werden mittlerweile in jedem Unternehmen personenbezogene Daten erhoben, verarbeitet oder gespeichert. Dabei kommt im Zuge der täglichen Email- und Internetnutzung auch dem internationalen Datentransfer immer mehr Bedeutung zu. In diesem Zusammenhang ist zu berücksichtigen, dass der Datentransfer in sog. unsichere Drittländer, zu denen nach Auffassung der EU-Kommission insbesondere auch die USA gehören, ohne ausreichende Sicherstellung eines angemessenen Datenschutzniveaus durch Vereinbarung der datenaustauschenden Unternehmen oder durch Einwilligungserklärung des Arbeitnehmers mit einer Geldbuße von bis zu € 250.000,00 geahndet werden kann (§ 43 BDSG).[6] Für den Fall vorsätzlichen und auf die Erzielung von Entgelt gerichteten Handelns sieht das Gesetz für bestimmte Fälle auch eine Freiheitsstrafe vor (§ 44 Abs. 1 BDSG).

Wird den Arbeitnehmern die private Nutzung von Telekommunikationseinrichtungen gestattet (vor allem Telefon, Email und Internet), sind neben den Vorschriften des BDSG auch die Vorgaben des Telekommunikationsgesetzes (TKG) zu berücksichtigen. Für die private E-mailkorrespondenz ist deshalb das Fernmeldegeheimnis zu beachten (§ 88 TKG). Eingehende Emails müssen auch dann grundsätzlich ungelesen an den Arbeitnehmer weitergeleitet werden, wenn die private Nutzung untersagt ist. Eine diesen Anforderungen genügende Organisation ist schon angesichts der Gefahren für die gesamte betriebliche EDV zur Verhinderung einer Verseuchung mit Viren unerlässlich. Auch insoweit sind Straf- und Bußgeldvorschriften zu beachten (§§ 148, 149 TKG).

---

6 Vgl. auch *Mengel/Hagemeister,* BB 2006, 2466, 2469 m.w.N.

1.7 Betriebsverfassungsrecht

Die Öffentlichkeitswirkung des Arbeitsrechts und die Bedeutung der arbeitsrechtlichen Compliance wurden in der jüngeren Vergangenheit nicht zuletzt vor dem Hintergrund der VW-Affäre um Lust- und Luxusreisen für Betriebsratsmitglieder unterstrichen. Auch – aber sicherlich nicht nur – mit Blick auf die strafrechtliche Relevanz der Begünstigung und Benachteiligung von Betriebsratsmitgliedern (§ 119 Abs. 1 Nr. 3 BetrVG) sowie die in diesen Fällen entstandenen Image-Schäden ist verstärkt auf die Einhaltung der betriebsverfassungsrechtlichen Vorgaben zu achten.[7] Ferner führt die Missachtung der betriebsverfassungsrechtlichen Beteiligungsrechte im Regelfall zur Unwirksamkeit der arbeitgeberseitigen Maßnahme. So ist etwa jede Kündigung ohne Beteiligung des Betriebsrats unwirksam. Insgesamt ist es daher dringend erforderlich, den Bereich der betrieblichen Mitbestimmung genauestens im Auge zu behalten und die betrieblichen Vorgänge auf entsprechende Konformität zu überprüfen.

2. Compliance Systeme

Führt man sich die vorstehend zusammengefassten wesentlichen Haftungsrisiken im Arbeitsrecht neben den in anderen Rechtsgebieten bestehenden Maßgaben vor Augen, dürfte ausreichend Anlass zur Einführung oder Verbesserung von Compliance Systemen in Unternehmen jeder Größe gegeben sein.

Welche Compliance Systeme geeignet sind, ist im konkreten Einzelfall zu entscheiden und dürfte im Ergebnis von der Größe und der (Personal-) Struktur des Unternehmens abhängig sein.

Während bei kleineren Unternehmen die Verteilung der den Arbeitgeber treffenden Aufgaben und Pflichten auf die Mitarbeiter unter Berücksichtigung eines klaren Organisationsaufbaus und unter Vermeidung paralleler Zuständigkeiten noch ausreichen dürfte, wird der Arbeitgeber in größeren Unternehmen zu weiter reichenden Maßnahmen greifen müssen. Dabei kommt Ethikrichtlinien oder Verhaltenskodizes in den Konzerngesellschaften US-amerikanischer Unternehmen eine besondere Bedeutung zu. Denn nach den Regelungen der US-amerikanischen Börsenaufsicht (Securities Exchange Commission – kurz „SEC" genannt) sind die dort notierten Unternehmen zur Einführung und Veröffentlichung eines „Code of Business Conduct and Ethics" verpflichtet.[8] Vor dem Hintergrund der Verschärfung der

---

[7] Vgl. auch *Mengel/Hagemeister,* BB 2006, 2466, 2469.

[8] Sec. 303 A Nr. 10 des New York Stock Exchange's Listed Company Manual.

Sanktionen durch den Sarbanes-Oxley-Act wird man hieraus eine faktische Pflicht zur Einführung von Ethikrichtlinien auch in den deutschen Konzernunternehmen ableiten müssen. In diesen Fällen kommt es dann aber unvermeidbar zu Schnittstellen zwischen den zwingenden Vorgaben der SEC und dem national ebenfalls zwingenden Arbeitsrecht. Denn gerade große Unternehmen legen besonderen Wert auf eine einheitliche weltweite Ausgestaltung ihrer Ethikrichtlinien. Dieser Aufgabe muss sich die Compliance Abteilung oder der Compliance Officer stellen.

Typischer Inhalt solcher Ethikrichtlinien sind dabei insbesondere: Verschwiegenheitsklauseln, Wertpapiertransaktionsklauseln zur Verhinderung von Insidergeschäften, Nebentätigkeitsklauseln, Regelungen zur Annahme von Geschenken, Verhalten in Geschäftsbeziehungen, sog. Whistleblowerklauseln (betr. die Pflicht zur Anzeige von Pflichtverstößen anderer Arbeitnehmer und den Umgang mit den erhaltenen Informationen / Informanten), aber auch Regelungen zum allgemeinen Verhalten der Mitarbeiter am Arbeitsplatz, Regelungen zum privaten Umgang der Arbeitnehmer untereinander[9] sowie dem Verbot verbaler Äußerungen etc.[10]

Ethikrichtlinien richten sich dabei an die Mitarbeiter des Arbeitgebers. Ob die Mitarbeiter sich an die dort aufgeführten Verhaltensvorgaben halten müssen, hängt davon ob, ob der Arbeitgeber diese mit verbindlicher Wirkung für den einzelnen Arbeitnehmer in das Arbeitsverhältnis eingeführt hat. Dabei kommen im Ergebnis drei Möglichkeiten zur Umsetzung in Betracht: Die Umsetzung durch Ausübung des arbeitgeberseitigen Direktionsrechts, die Vereinbarung im Arbeitsvertrag oder die Regelung in einer Betriebsvereinbarung.

2.1 Einführung kraft arbeitgeberseitigen Direktionsrechts

Das arbeitgeberseitige Direktionsrecht ist in § 106 Gewerbeordnung (GewO) normiert. Hiernach kann der Arbeitgeber Inhalt, Ort und Zeit der Arbeitsleistung nach billigem Ermessen näher bestimmen soweit diese Arbeitsbedingungen nicht durch den Arbeitsvertrag, Bestimmungen einer Betriebsvereinbarung, eines anwendbaren Tarifvertrags oder gesetzliche Vorschriften festgelegt sind. Dies gilt ausdrücklich auch hinsichtlich der Ordnung und des Verhaltens der Arbeitnehmer im Betrieb.

Aus Arbeitgebersicht ist die Einführung von Verhaltensvorgaben in Ethikrichtlinien durch einseitige Weisung die reizvollste Lösung. Wie sich aber bereits aus § 106 GewO ergibt, sind den Weisungen des Arbeitgebers zum Teil enge Grenzen gesetzt. Denn das Direktionsrecht

---

9 Vgl. die Wal-Mart-Entscheidung zum “Flirtverbot”: LAG Düsseldorf v. 14.11.2005 – 10 TaBV 46/05, NZA-RR 2006, 81 f.

10 Vgl. hierzu *Meyer*, NJW 2006, 3605, 3607 m.w.N.

kann nur dann greifen, wenn bereits bestehende vertragliche oder gesetzliche Haupt- oder Nebenpflichten konkretisiert werden sollen. Neue Pflichten können durch das Direktionsrecht ebenso wenig zum Gegenstand des Arbeitsverhältnisses gemacht werden wie Pflichten, die vom Arbeitsvertrag, einer Betriebsvereinbarung, einem Tarifvertrag oder gesetzlichen Vorschriften abweichen.

Unterteilt man darüber hinaus die in Ethikrichtlinien regelmäßig enthaltenen Verhaltensvorgaben in die folgenden drei Kategorien:

- Regelungen mit ausschließlichem Tätigkeitsbezug
- Regelungen mit Bezug auf die Tätigkeit und das sonstige Verhalten und
- Regelungen zum außerdienstlichen und privaten Verhalten[11]

wird deutlich, dass zumindest Vorgaben zur dritten Kategorie nur in eng begrenzten Ausnahmefällen Gegenstand des Weisungsrechts sein können. Dies dürfte im Ergebnis nur dann möglich sein, wenn eine sich aus dem Arbeitsvertrag ergebende Nebenpflicht konkretisiert werden soll (z. B. Nebentätigkeitsverbote, Wertpapiertransaktionsklauseln mit Verboten für den Arbeitnehmer und seine Familienangehörigen oder das Verbot, außerdienstlich so viel Alkohol zu trinken, dass später die Arbeit beeinträchtigt wird).

Hiervon abgesehen lassen sich indes schon mit Blick auf die ersten beiden Kategorien durchaus zahlreiche compliance-relevante Sachverhalte durch das Direktionsrecht in das Arbeitsverhältnis einführen, die im Wesentlichen jedoch nur Hinweise auf gesetzlich ohnehin bestehende Anforderungen enthalten. Hierzu zählen insbesondere die Vorgaben zur Einhaltung der Wertpapierhandelsrechtsregeln, der Regeln des Steuer- und Sozialversicherungsrechts, aber auch etwa die Pflicht zur Verschwiegenheit im Geschäftsverkehr, zum Schutz von Betriebs- und Geschäftsgeheimnissen sowie dem Verbot der Annahme von Geschenken etc.[12]

Werden Verhaltensvorgaben in Form von Ethikrichtlinien durch Weisungsrecht des Arbeitgebers in das Arbeitsverhältnis eingeführt, ist aus Arbeitgebersicht darüber hinaus ein schriftliches Empfangsbekenntnis unverzichtbar. Denn bei Weisungen handelt es sich um empfangsbedürftige Willenserklärungen, die nur durchgesetzt werden können, wenn sie dem Arbeitnehmer nachweislich bekannt gemacht worden sind.[13]

2.2 Einführung durch Individualvereinbarung

Rechtssicherer ist die Umsetzung von Verhaltensvorgaben durch eine mit dem Arbeitnehmer getroffene Vereinbarung. Im Rahmen der Vertragsfreiheit sind auch deutlich weitergehende

---

11 Vgl. *Borgmann*, NZA 2003, 352, 353.
12 *Mengel/Hagemeister*, NZA 2007, 1386, 1387.
13 Vgl. hierzu *Borgmann*, NZA 2003, 352, 354.

Vereinbarungen möglich als dies dem Arbeitgeber einseitig kraft Direktionsrechts offen steht. Auch einer solchen Vereinbarung sind indes Grenzen gesetzt. Insbesondere dürfen Vereinbarungen nicht sittenwidrig sein oder gegen Treu und Glauben verstoßen. Hinzu kommt, dass vorformuliere Arbeitsvertragsbedingungen der Inhaltskontrolle nach §§ 305 ff. BGB unterliegen. Verhaltensvorgaben dürfen die Arbeitnehmer mithin nicht unangemessen benachteiligen. Dabei kann davon ausgegangen werden, dass die Anforderungen an die Rechtmäßigkeit steigen, je weiter die Verhaltensvorgaben von der eigentlichen Arbeitspflicht entfernt sind und auf das allgemeine Verhalten des Arbeitnehmers einwirken. Insbesondere Pflichten der unter der vorstehenden Ziffer 1 genannten zweiten und dritten Kategorie bedürfen mithin einer konkreten Begründung, um den Eingriff in die Privatsphäre zu rechtfertigen.[14]

Losgelöst hiervon ist zu berücksichtigen, dass die einzelvertragliche Einbeziehung von Verhaltensvorgaben in der Praxis wohl nur selten umfassend möglich ist. Zwar wird man davon ausgehen können, dass eine vertragliche Regelung bei Neueinstellungen noch problemlos umgesetzt werden kann. Im laufenden Arbeitsverhältnis besteht indes das Risiko, dass der Arbeitnehmer einer Einbeziehung in den Arbeitsvertrag nicht zustimmt – dies gilt insbesondere bei weit reichenden Vorgaben für den außerdienstlichen und privaten Bereich. In einem solchen Fall bliebe alleine die (wohl nur theoretische) Möglichkeit, die Verhaltensvorgaben durch Änderungskündigung gemäß § 2 KSchG zum Inhalt des Arbeitsverhältnisses zu machen.

2.3 Einführung durch Betriebsvereinbarung

Schließlich können Verhaltensvorgaben in Betrieben mit Arbeitnehmervertretung auch durch Betriebsvereinbarung in das Arbeitsverhältnis eingeführt werden. Teils ist dies obligatorisch. Die Umsetzung durch Betriebsvereinbarung ist nämlich immer dann zwingend erforderlich, wenn der Betriebsrat mit Blick auf den Regelungsgehalt der einzelnen Klausel des Verhaltenskodexes oder der Ethikrichtlinie ein Mitbestimmungsrecht hat. Richtigerweise sind Ethikrichtlinien weder allgemein mitbestimmungspflichtig noch pauschal mitbestimmungsfrei.[15]

Dreh- und Angelpunkt der mitbestimmungspflichtigen Tatbestände ist insoweit § 87 Abs. 1 Nr. 1 BetrVG. Hiernach sind mitbestimmungspflichtig die Maßnahmen des Arbeitgebers, die das Ordnungsverhalten der Arbeitnehmer im Betrieb betreffen. Hierunter fallen z. B. Alkohol- oder Rauchverbote, Regelungen zur Einrichtung von sog. Chinese Walls bei Finanzunternehmen, Kleiderordnungen oder Vorgaben zur Nutzung von Email/Internet sowie Whistleblower-Hotlines, wobei bei letzteren zum Teil ein Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG hergeleitet wird.[16] Nicht mitbestimmungspflichtig sind hingegen Maßnahmen oder

---

[14] *Meyer*, NJW 2006, 3605, 3608.

[15] *Mengel/Hagemeister*, BB 2007, 1386, 1392.

[16] ArbG Wuppertal v. 15.6.2005 – 5 BV 20/05, NZA-RR 2005, 476-481.

Regelungen, die das Arbeitsverhalten betreffen. Hierunter fallen alle arbeitgeberseitigen Maßnahmen, die bestimmen, welche Arbeiten und vor allem in welcher Art und Weise sie auszuführen sind.[17] Erst recht besteht kein Mitbestimmungsrecht des Betriebsrats bei Maßnahmen, die das außerdienstliche oder private Verhalten der Arbeitnehmer betreffen.

Will der Arbeitgeber umfassende Verhaltensvorgaben in seinem Unternehmen einführen, die neben mitbestimmungsfreien auch mitbestimmungspflichtige Regelungen enthalten, müssen zumindest die mitbestimmungspflichtigen Regelungen durch Betriebsvereinbarung umgesetzt werden. Ob daneben auch die mitbestimmungsfreien Regelungen freiwillig in die Betriebsvereinbarung aufgenommen werden oder insoweit auf die vorgenannten Möglichkeiten der Einführung kraft Direktionsrechts oder durch einzelvertragliche Regelung zurückgegriffen werden soll, ist eine Entscheidung des konkreten Einzelfalls und kann nicht abschließend bewertet werden.

Der Vorteil der Einführung / Umsetzung per Betriebsvereinbarung liegt sicherlich darin, dass gemeinsam mit der Arbeitnehmervertretung eingeführte Ethikrichtlinien auf eine größere Akzeptanz bei den Arbeitnehmern selbst stoßen dürften. Auch hat der Arbeitgeber den Vorteil, dass er nur einen Ansprech- und Verhandlungspartner für die Ausgestaltung der Regelungen hat. Insbesondere in großen Unternehmen empfiehlt sich daher oftmals eine Umsetzung kraft Betriebsvereinbarung. Dabei versteht sich von selbst, dass auch die in Betriebsvereinbarungen geregelten Verhaltensvorgaben nicht gegen zwingendes Recht, insbesondere die Grundrechte des Arbeitnehmers (z. B. Verbot der Liebesbeziehung zwischen Mitarbeitern) verstoßen dürfen.

3. Ausblick/Aktuelle Fragestellungen

Wirksame Compliance Systeme werden vor dem Hintergrund der zunehmenden Vereinheitlichung weltweiter Konzernvorgaben immer mehr an Bedeutung gewinnen. Dabei ist der Arbeitgeber gut beraten, frühzeitig zu überlegen, in welchem Umfang den Mitarbeitern Compliance Pflichten auferlegt werden und wie diese konkret in das einzelne Arbeitsverhältnis eingeführt werden, um auch tatsächlich verbindliche Wirkung zu erlangen.

Wichtiger Bestandteil von Compliance Systemen ist neben der Einführung von Verhaltensvorgaben durch Ethikrichtlinien oder Verhaltenskodizes aber auch die ständige Kontrolle der Compliance Systeme. Zu diesem Zweck werden in vielen Unternehmen bereits sog. Compliance Officer oder – mit zunehmender Größe des Unternehmens – ganze Compliance Abteilungen beschäftigt. Diese haben die Verantwortung für das jeweilige Compliance System inne und berichten der Geschäftsleitung, agieren dabei aber grundsätzlich unabhängig und weisungsfrei.

---

[17] Fitting, BetrVG, 23. Aufl. 2006 § 87 Rz 65.

An die damit in der Praxis bereits vielfach umgesetzten Compliance Strukturen schließen sich weitere Fragen an. Dies gilt insbesondere für die Frage, in wessen Interesse z. B. der Compliance Officer tätig wird. Ähnlich der Funktion eines Datenschutz- oder Strahlenschutzbeauftragten ist hier zu überlegen, inwieweit der Compliance Officer im öffentlichen Interesse oder im betrieblichen Interesse tätig wird. Die Antwort auf diese Frage wird insbesondere für die Ausgestaltung seiner Unabhängigkeit von Bedeutung sein. Daneben ist von Fall zu Fall zu entscheiden, wie genau der Anstellungsvertrag eines Compliance Officers ausgestaltet wird, um seiner Funktion gerecht zu werden. Wem etwa ist er unterstellt? Welche konkreten Regelungen sind in den Anstellungsvertrag aufzunehmen, ohne dass seine unabhängige Stellung beeinträchtigt wird?

Nach alledem hat das Arbeitsrecht als wichtiger Bestandteil der Compliance zu gelten. Denn nur über das Arbeitsrecht kann Compliance überhaupt verbindlich in ein deutsches Unternehmen eingeführt werden. Noch längst sind nicht alle Fragen hierzu geklärt. Ziel muss daher aus Arbeitgebersicht vorrangig sein, Sensibilität für die Compliance unter arbeitsrechtlichen Gesichtspunkten zu entwickeln.

Stichwortverzeichnis

B

C

D

H

I

J

K

L

M

N

O

P

Q

R